Contrato que celebran en esta ciudad de Guadalajara, Jalisco, el día **20 del mes de julio del año 2026**, la **Secretaría de Administración** del Poder Ejecutivo del Estado de Jalisco, a la que en lo sucesivo se le denominará como la **"SECRETARÍA"**, la cual es representada en este acto por **Acuerdo Delegatorio del Secretario de Administración número SECADMON/ACU/01/2026**; por el **Lic. Jesús Ezequiel Martínez Nieto**, **Director Ejecutivo y Padrón de Proveedores**, acompañada de la dependencia requirente, la **Secretaría de administración** del Poder Ejecutivo del Estado de Jalisco, a la que en lo sucesivo se le denominará como la **"DEPENDENCIA"**, representada en este acto por la **Lic. Stephanie Viridiana Carrillo**, en su carácter de **Directora Administrativa**; y **BEEHIVE SYSTEMS, S.A. DE C.V.,** a quien en lo subsecuente se le denominará como el **"PROVEEDOR"**, representada en este acto por el **C. Ariel Cárdenas Peña**; y cuando se refiera a ambos contratantes se les denominará como las **"PARTES"**, las cuales llevan a cabo las siguientes:

D E C L A R A C I O N E S

I. Declara el representante de la "SECRETARÍA" que:

a) Que la **"SECRETARÍA"** es la dependencia de la Administración Pública Estatal competente para representar al Poder Ejecutivo del Estado de Jalisco en las adquisiciones de bienes, productos y servicios, en atención a lo dispuesto por los artículos 2, numeral 2, 3, numeral 1, fracción I, 5, numeral 1, fracción I, 7, numeral 1, fracción III, 14, numeral 1, 15, numeral 1, fracción I, 16, numeral 1, fracción III, y 19, numeral 1, fracción XI, de la Ley Orgánica del Poder Ejecutivo del Estado de Jalisco, así como por los artículos 34, 35 y 36 de la Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios, en lo subsecuente la **"LEY",** en relación al artículo 3 del Reglamento de la Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios, en lo subsecuente el **"REGLAMENTO"**.

b) Que su representante cuenta con las facultades para llevar a cabo las operaciones de compra requeridas por las dependencias de la administración pública centralizada del Poder Ejecutivo del Estado, y consecuentemente para contratar y obligarse a nombre del Gobierno del Estado de Jalisco, de conformidad con los artículos 2, fracción XII, 9, fracción II, 13, fracción X, 19, fracciones V, X y XV, 23 fracción X, 41 fracción X y 44 fracciones VII, X, XI y XIX, del Reglamento Interno de la Secretaría de Administración del Estado de Jalisco; así como los artículos 4 y 12, del "**REGLAMENTO"**.

c) Que mediante Acuerdo **SECADMON/ACU/01/2026**, de fecha 17 de marzo del 2026; el **C. Rafael Orendain Parra**, en su carácter de **Secretario de Administración**, delega al **Lic. Jesús Ezequiel Martínez Nieto**, **Director Ejecutivo y Padrón de Proveedores** de la **"SECRETARÍA"**, las facultades, atribuciones y obligaciones correspondientes para llevar a cabo la suscripción de los instrumentos jurídicos y **actuaciones administrativas** relativos a los procedimientos de contratación para las áreas organizativas de la Secretaría de Administración y de la Administración Pública Centralizada del Poder Ejecutivo del Estado de Jalisco, lo anterior, de conformidad a los artículos 7 fracción XVII y 19 fracción X, del Reglamento Interno de la Secretaría de Administración.

d) Que la **Lic. Stephanie Viridiana Carrillo**, en su carácter de Directora Administrativa de la **"SECRETARÍA"**, cuenta con las facultades para solicitar la adquisición de los bienes, productos y/o servicios que requieran las áreas organizativas de la **"SECRETARÍA"** para su funcionamiento, de conformidad con los artículos 2, fracción XII, 5, fracción II, 7, fracción XVII, del Reglamento Interno de la Secretaría de Administración del Estado de Jalisco.

e) Que para efectos del presente, cuando en la **"LEY"**, así como en el **"REGLAMENTO"**, se haga mención a la Subsecretaría de Administración, se entenderá que se refieren a la Secretaría de Administración del Poder Ejecutivo del Estado de Jalisco, toda vez que ciertas facultades y atribuciones de la antes Secretaría de Planeación, Administración y Finanzas se establecieron a cargo de esta última, de conformidad con los artículos Primero, Quinto y Décimo Transitorios de la Ley Orgánica del Poder Ejecutivo del Estado de Jalisco, publicada en el Periódico Oficial "El Estado de Jalisco" el 5 de diciembre de 2018.

f) Que de conformidad con el artículo 41 de la Ley General de Contabilidad Gubernamental, y con el inciso D, numeral 1, punto 15, del Clasificador por Fuentes de Financiamiento, publicado en el Diario Oficial de la Federación el 2 de enero de 2013 y reformado el 20 de diciembre de 2016, el Estado está facultado para contratar, por lo que las facultades descritas en líneas anteriores aplican para comparecer a la firma del presente instrumento.

g) Que para los efectos del presente contrato señala como domicilio el ubicado en Prolongación Avenida Alcalde número 1221, colonia Miraflores, zona Centro, C.P. 44270 de esta ciudad de Guadalajara, Jalisco, México; mientras que para **efectos de facturación** su domicilio es la calle Pedro Moreno No. 281, Guadalajara Centro, Guadalajara, Jalisco, C.P. 44100, y su R.F.C. es **SPC130227L99**.

JALISCO
GOBIERNO DEL ESTADO

Av. Fray Antonio Alcalde #1221,
Col. Miraflores, Guadalajara, Jalisco.
C.P. 44270 | 33 3818 2800

II. Declara el representante del "PROVEEDOR" bajo protesta de decir verdad:

a) Que es una Sociedad de Anónima de Capital Variable, legalmente constituida e integrada conforme a las legislaciones que le son aplicables, según consta en el testimonio de la Escritura Pública número 83,127 de fecha 11 de septiembre del 2020, otorgada ante la fe del Lic. Roberto Armando Orozco Alonzo, Notario Público Titular número 130, en Guadalajara, Jalisco, misma que se encuentra inscrita en el Registro Público de la Propiedad y de Comercio del Estado de Jalisco, bajo el folio mercantil electrónico número **N-2020060229**, en la que se contienen los estatutos, objeto y demás elementos de la constitución legal de la empresa denominada **BEEHIVE SYSTEMS, S.A. DE C.V.**

b) Que el **C. Ariel Cárdenas Peña**, en su carácter de Presidente del Consejo de Administración, tiene las facultades jurídicas necesarias vigentes y suficientes para suscribir el presente contrato tal y como se advierte en el testimonio de la Escritura Pública número 83,127 de fecha 11 de septiembre del 2020, otorgada ante la fe del Lic. Roberto Armando Orozco Alonzo, Notario Público Titular número 130, en Guadalajara, Jalisco, misma que se encuentra inscrita en el Registro Público de la Propiedad y de Comercio del Estado de Jalisco, bajo el folio mercantil electrónico número **N-2020060229**, quien se identifica con su credencial para votar vigente, expedida por el Instituto Nacional Electoral número [redacted] 1

c) Quien suscribe manifiesta bajo protesta de decir verdad que cuenta con las facultades jurídicas necesarias, vigentes y suficientes para contraer derechos y obligaciones en nombre del **"PROVEEDOR",** mismas que no le han sido revocadas, modificadas o limitadas en forma alguna.

d) Que conforme a lo dispuesto en los artículos 17 y 20 de la **"LEY"**, su representada se encuentra debidamente inscrita y actualizada ante el Registro Único de Proveedores y Contratistas del Estado de Jalisco, bajo el número de registro de proveedor **P37430**, y que la información contenida en el expediente respectivo no ha sufrido modificación alguna y se encuentra vigente.

e) Que señala como domicilio fiscal y convencional de su representada, para los fines de este contrato, así como para recibir todo tipo de citas y notificaciones, el ubicado en la calle Juan Palomar y Arias No. 118, colonia Vallarta Norte, ciudad de Guadalajara, estado de Jalisco, C.P. 44690, el teléfono 3319897121 y el correo electrónico administracion@beehivesystems.mx.

f) Que cuenta con Registro Federal de Contribuyentes **BSY200921LL1**.

g) Que tiene la capacidad legal, financiera, técnica y productiva necesaria para dar cumplimiento al presente contrato.

h) Que tiene la aprobación y los permisos correspondientes de las autoridades competentes y en caso de aplicar, cuenta con los derechos de propiedad industrial e intelectual, necesarios para la prestación de los servicios y abastecimientos del o los productos contratados.

i) Que conoce el contenido de los requisitos que establece la **"LEY"**, así como el contenido de las Bases de la Licitación Pública Local número **LPL 334/2026 con concurrencia del Comité**, ***"PÓLIZA DE DESARROLLO, MANTENIMIENTO Y SOPORTE A LOS SISTEMAS Y PROCESOS INFORMÁTICOS CON FÁBRICA DE SOFTWARE"***, misma que protesta cumplir.

j) Que no se encuentra en ningún supuesto de los establecidos en el artículo 52 de la **"LEY"**.

k) Que conoce y se obliga a cumplir con el Convenio 138 de la Organización Internacional del Trabajo en materia de erradicación del Trabajo Infantil, del artículo 123 Constitucional, apartado A) en todas sus fracciones y de la Ley Federal del Trabajo en su artículo 22, manifestando que ni en sus registros, ni en su nómina tiene empleados menores de quince años y que en caso de llegar a tener a menores de dieciocho años que se encuentren dentro de los supuestos de edad permitida para laborar le serán respetados todos los derechos que se establecen en el marco normativo transcrito.

l) Manifiesta estar al corriente en los pagos que se derivan de sus obligaciones fiscales, en específico de las previstas en el artículo 32-D del Código Fiscal Federal vigente, así como de sus obligaciones fiscales en materia de seguridad social, ante el Instituto del Fondo Nacional de la Vivienda para los Trabajadores y el Instituto Mexicano del Seguro Social.

III. Las "PARTES" declaran:

a) Que el presente contrato, cuyo objeto será solventado con **RECURSOS FISCALES NO ETIQUETADOS DEL EJERCICIO FISCAL 2026**, se originó con motivo de la Licitación Pública Local número **LPL 334/2026 con concurrencia del Comité** denominada ***"PÓLIZA DE DESARROLLO, MANTENIMIENTO Y SOPORTE A LOS SISTEMAS Y PROCESOS INFORMÁTICOS CON FÁBRICA DE SOFTWARE"***, la cual fue resuelta o autorizada a favor del **"PROVEEDOR"** de conformidad con el fallo de adjudicación de fecha **20** de **julio**

JALISCO
GOBIERNO DEL ESTADO
Av. Fray Antonio Alcalde #1221,
Col. Miraflores, Guadalajara, Jalisco.
C.P. 44270 | 33 3818 2800

del **2026**, emitido por el **Comité de Adquisiciones de la Administración Publica Centralizada del Poder Ejecutivo del Estado de Jalisco** de la **"SECRETARÍA"**.

b) Que el **"PROVEEDOR"** se obliga a cumplir con las bases publicadas respecto de la licitación señalada en el inciso que antecede y su junta aclaratoria, así como el fallo de adjudicación, en los cuales se detallan las características del servicio de la póliza objeto de este contrato.

c) Que, para efectos del presente instrumento, las referencias que se hagan a la **"LEY"**, se entenderán hechas a la Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.

d) Que se reconocen recíprocamente el carácter con el que comparecen y sujetan el presente contrato al tenor de las siguientes:

C L Á U S U L A S

PRIMERA.- DEL OBJETO. En virtud del presente contrato, la **"SECRETARÍA"** adquiere del **"PROVEEDOR"** "*póliza de desarrollo, mantenimiento y soporte a los sistemas y procesos informáticos con fábrica de software*", en adelante el servicio, cuyas características, cantidades, precios y descripción se describen en el Fallo de Adjudicación, los cuales se transcriben a continuación:

Partida	Cantidad	U.M.	Descripción	P.U.	Importe
1	1	Servicio(s)	Póliza de Desarrollo, Mantenimiento y Soporte a los Sistemas y Procesos Informáticos con Fabrica de Software.	$52,532,738.85	$52,532,738.85
				Subtotal	**$52,532,738.85**
				I.V.A.	**$8,405,238.22**
				Total	**$60,937,977.07**

SEGUNDA.- DE LA PRESTACIÓN DEL SERVICIO. El **"PROVEEDOR"** deberá entregar la póliza objeto de este contrato de forma inmediata, en una sola exhibición a partir de la emisión del fallo de adjudicación siendo dicha entrega en el Almacén de Parcialidades de la **"SECRETARIA"** con domicilio en Prolongación Avenida Alcalde número 1221, colonia Miraflores, zona Centro, C.P. 44266 de esta ciudad de Guadalajara, Jalisco, México, llevándose a cabo, bajo la estricta responsabilidad del proveedor, sujetándose a lo señalado en la totalidad de las especificaciones técnicas contenidas en su propuesta, la cual fue aprobada en la Licitación descrita en líneas anteriores, haciendo la acotación que dicha póliza tendrá una cobertura de 12 meses a partir de la firma del presente instrumento jurídico.

Dada la naturaleza del presente contrato y con fin simplificativo, los servicios adquiridos consistirán en lo plasmado en la **propuesta técnica** del proveedor, la cual, para el cumplimiento de las obligaciones derivadas del presente instrumento, forma parte integral del mismo como **anexo único.**

TERCERA.- DE LA VIGENCIA. La vigencia del presente instrumento contractual comenzará a correr a partir del día **20 del mes de julio del año 2026**, y concluirá el día **20 del mes de julio del año 2027**, a excepción de las garantías, las cuales seguirán surtiendo sus efectos hasta el término de su vigencia.

CUARTA.- DEL PRECIO. El **"PROVEEDOR"** fija un precio por la cantidad de **$60,937,977.$\underline{07}$ M.N. (sesenta millones novecientos treinta y siete mil novecientos setenta y siete pesos $^{07}/_{100}$ Moneda Nacional)** Impuesto al Valor Agregado incluido, por los servicios objeto de este contrato.

QUINTA.- DE LA FORMA DE PAGO. La Secretaría de la Hacienda Pública realizará el pago al **"PROVEEDOR"** en moneda nacional, mediante pago único o en parcialidades. De igual manera, se hace la acotación de que el **"PROVEEDOR"** requiere que se le efectúe pago de anticipo, siendo del **50%** cincuenta por ciento del monto total de la orden de compra, de acuerdo al artículo 78 de la **"LEY"**. El pago correspondiente se efectuará dentro de los 30 treinta días naturales siguientes a aquel en que la documentación señalada a continuación para el pago parcial o total, así como para el pago del anticipo, sea recibida en la Dirección de Almacenes de la **"SECRETARÍA":**

Documentos para el pago de anticipo:

a) Original y copia del comprobante fiscal respectivo expedido a favor de la Secretaría de la Hacienda Pública, cuyo domicilio es en la calle Pedro Moreno No. 281, Guadalajara Centro, Guadalajara, Jalisco, C.P. 44100, y su R.F.C. es SPC130227L99.
b) Impresión de la verificación del CFDI de la página del Servicio de Administración Tributaria.
c) Original del contrato.

JALISCO
GOBIERNO DEL ESTADO

Av. Fray Antonio Alcalde #1221,
Col. Miraflores, Guadalajara, Jalisco.
C.P. 44270 | 33 3818 2800

d) Copia de la Declaración de aportación del 5 al millar para el Fondo Impulso Jalisco (**ANEXO 7** de las bases) en la cual el **"PROVEEDOR"** declara que **NO** es su voluntad de realizar la aportación del 5 al millar del monto total del contrato antes del I.V.A., para su entero al Fondo Impulso Jalisco.
e) Original de la póliza de fianza de anticipo a la que se hace referencia en la cláusula **SÉPTIMA bis** de este contrato, expedida por una institución mexicana legalmente autorizada.

Documentos para cada pago parcial o total:

a) Original y copia del comprobante fiscal respectivo expedido a favor de la Secretaría de la Hacienda Pública, cuyo domicilio es en la calle Pedro Moreno No. 281, Guadalajara Centro, Guadalajara, Jalisco, C.P. 44100, y su R.F.C. es SPC130227L99. validado por la **"SECRETARIA"**
b) Impresión de la verificación del CFDI de la página del Servicio de Administración Tributaria.
c) 1 copia del contrato.
d) Oficio de Recepción a Entera Satisfacción.
e) Copia de la Declaración de aportación del 5 al millar para el Fondo Impulso Jalisco (**ANEXO 7** de las bases) en la cual el **"PROVEEDOR"** declara que **NO** es su voluntad realizar la aportación del 5 al millar del monto total del contrato antes del I.V.A., para su entero al Fondo Impulso Jalisco.
f) 1 copia de la garantía de cumplimiento a la que se hace referencia en la cláusula **SÉPTIMA** de este contrato.

De ser el caso, de acuerdo con los artículos 76 y 77 de la Ley del Presupuesto, Contabilidad y Gasto Público del Estado de Jalisco, los pagos que se tengan que efectuar con cargo a ejercicios presupuestales futuros, estarán sujetos a la aprobación del presupuesto correspondiente.

SEXTA.- DEL PRECIO FIRME. El **"PROVEEDOR",** se compromete a sostener el precio de los productos y/o servicios de la póliza prestados durante la vigencia de este contrato, así como de ser procedente, el precio unitario por unidad de medida de lo que se compromete a ejecutar, de no hacerlo, por cualquier motivo, la **"SECRETARÍA"**, podrá rescindir, sin necesidad de declaración judicial, la contratación, sin responsabilidad para el mismo, y ejecutar las garantías otorgadas por el cumplimiento del contrato, y en su caso la de aplicación y amortización del anticipo, independientemente de ejercer las acciones legales correspondientes para que el **"PROVEEDOR"** cubra los daños y perjuicios ocasionados.

SÉPTIMA.- DE LA GARANTÍA PARA EL CUMPLIMIENTO DE LAS OBLIGACIONES. El **"PROVEEDOR"** se obliga a entregar dentro de los 15 días hábiles siguientes a la firma del presente contrato, una garantía que responda por el cumplimiento de las obligaciones del presente contrato, así como por la calidad de los servicios prestados, a favor de la Secretaría de la Hacienda Pública, la cual podrá ser a través de cheque certificado o de caja, en efectivo mediante billete de depósito tramitado ante la Recaudadora N° 000 o mediante fianza expedida por una institución mexicana legalmente autorizada, por el importe del 10% diez por ciento del monto total del contrato, con una vigencia a partir del día de la fecha de la firma del contrato y hasta por 12 meses posteriores a partir de su terminación, con el fin de garantizar el cumplimiento de este instrumento y la calidad del objeto del mismo. El **"PROVEEDOR"** está obligado a modificar la garantía descrita en la presente cláusula, en caso de convenio modificatorio, prórroga o adendum. Todo lo anterior de conformidad con el artículo 84 de la **"LEY"**.

La garantía para el cumplimiento de las obligaciones otorgada por el **"PROVEEDOR"**, podrá ser exigible y aplicada en cualquier tiempo en caso de que exista mala calidad en el objeto de este contrato, o por cualquier incumplimiento en las obligaciones en él establecidas, y será independiente de las acciones que deban ejercitarse por los daños y perjuicios que se originen con motivo del incumplimiento en cualquiera de las obligaciones contraídas por parte del **"PROVEEDOR"** de conformidad con lo dispuesto por el artículo 84, fracción I, de la **"LEY"**, y 107 de su **"REGLAMENTO"**.

SÉPTIMA bis.- DE LA FIANZA PARA LA CORRECTA APLICACIÓN DEL ANTICIPO. En caso de requerir anticipo, el **"PROVEEDOR"** se obliga a entregar dentro de los próximos 15 días hábiles, una garantía que responda por la correcta aplicación del anticipo a favor de la Secretaría de la Hacienda Pública, a través de fianza expedida por una institución mexicana legalmente autorizada, por el importe del 100% cien por ciento del monto total del anticipo y con una vigencia a partir de la firma del presente contrato y hasta en tanto se amortice el anticipo señalado en el mismo o este sea devuelto, con el fin de garantizar por la totalidad del monto del anticipo referida en este instrumento.

La fianza para la correcta aplicación del anticipo, otorgada por el **"PROVEEDOR"**, podrá ser exigible y aplicada en cualquier tiempo para la debida inversión o devolución total del mismo, en caso de presentarse defectos o mala calidad en el objeto del presente contrato, así como por cualquier incumplimiento en las obligaciones establecidas en este contrato, y será independiente de las acciones que deban ejercitarse por los daños y perjuicios que se originen con motivo del incumplimiento en cualquiera de las obligaciones contratadas por parte del **"PROVEEDOR"** de conformidad con lo dispuesto por el artículo 84, fracción II, de la **"LEY"**, y 107 de su **"REGLAMENTO"**.

OCTAVA.- DE LA GARANTÍA DE LA PRESTACIÓN DEL SERVICIO. El **"PROVEEDOR"** garantiza por 12 meses a partir del fallo de la licitación, en servicios, licencias y mano de obra. Así mismo, el **"PROVEEDOR"** garantiza la

JALISCO
GOBIERNO DEL ESTADO
Av. Fray Antonio Alcalde #1221,
Col. Miraflores, Guadalajara, Jalisco.
C.P. 44270 | 33 3818 2800

calidad del servicio de la póliza objeto de este contrato contra daños y defectos por el periodo que, entre las **"PARTES"** se determine, en el entendido de que lo prestará con la mejor calidad, diligencia y con personal calificado a efecto de cumplir con las especificaciones requeridas por la **"SECRETARÍA".**

NOVENA.- DE LA PENALIZACIÓN POR ATRASO EN EL SERVICIO. En caso que el **"PROVEEDOR"** no preste en tiempo y forma el servicio de la póliza objeto del presente contrato, por cualquier causa que no sea imputable a la **"SECRETARÍA"**, esta última podrá descontar al **"PROVEEDOR"**, de la cantidad establecida en la cláusula **CUARTA**, el 3% cuando el atraso se encuentre de 1 a 10 días naturales, el 6% cuando el atraso se encuentre de 11 a 20 días naturales, y el 10% cuando el atraso se dé de 21 a 30 días naturales, el cual se hará aplicable sobre el pago parcial y/o total, según sea el caso.

La **"SECRETARÍA"**, aplicará la penalización que corresponda en el caso de atraso en la prestación o rescindirá el contrato a causa del incumplimiento en la prestación de los servicios de la póliza en el término y/o condiciones establecidas en el contrato y/o orden de compra, dentro del plazo que se le conceda al **"PROVEEDOR"** a razón de cualquier prórroga o modificación, lo anterior de manera independiente a las acciones que deban ejercitarse por los daños y perjuicios que se originen con motivo del incumplimiento en cualquiera de las obligaciones contratadas por parte del **"PROVEEDOR"** de conformidad con lo dispuesto por el artículo 107 del **"REGLAMENTO"** de la **"LEY"**.

Si en cualquier momento en el curso de la ejecución del servicio de la póliza, el **"PROVEEDOR"** se encontrara en una situación que impidiera la oportuna entrega de los servicios por causas necesariamente justificadas, éste deberá notificar de inmediato al área requirente por escrito las causas de la demora y su duración probable, solicitando, en su caso, prórroga para su regularización, mínimo 3 días hábiles anteriores al vencimiento del plazo de entrega pactado en la orden de compra y/o contrato, esto con la finalidad de que el área requirente realice la valoración de la petición, para que en caso de no tener inconveniente esta misma solicite llevar a cabo la prórroga a la Dirección General de Abastecimientos, lo anterior con fundamento en el artículo 80 punto 1 de la **"LEY"**, y artículo 103 de su **"REGLAMENTO"**; en caso de no ser contestada la prórroga o se conteste de forma negativa se estará a lo dispuesto en el presente numeral en cuanto a los términos y aplicación de la penalización que corresponda.

En caso de que alguna de las obligaciones a cargo del **"PROVEEDOR"** no se presten de acuerdo a la forma y características convenidas, así como en cualquier caso exista falta de calidad en general de los servicios de la póliza prestados cualquier tipo de daño así como por el rechazo de los mismos el **"PROVEEDOR"** se obliga a cubrir como pena convencional la cantidad equivalente al 10% del monto total del contrato, independientemente del cumplimiento forzoso y/o de la rescisión del contrato que en su momento considere exigir la **"SECRETARÍA"** por los supuestos señalados.

El **"PROVEEDOR"** adjudicado se obliga a devolver las cantidades pagadas con los intereses correspondientes conforme a una tasa igual a la aplicada para prórroga en el pago de Créditos Fiscales según lo establece la Ley de Ingresos y el Código Fiscal, ambos del Estado de Jalisco, cuando la **"SECRETARÍA"**, determine que el (los) servicio(s) prestado(s) presenten falta de calidad en general, sea(n) prestado(s) con diferentes especificaciones a las solicitadas, por no cumplir con el fin para el cual fue(ron) contratado(s) o por ser prestado(s) fuera del término establecido.

DÉCIMA.- OBLIGACIONES DE LAS "PARTES".

La **"SECRETARÍA"**, tendrá las siguientes obligaciones:

- **a)** Otorgar todas las facilidades necesarias, a efecto de que el **"PROVEEDOR"** lleve a cabo el servicio de la póliza en los términos convenidos.
- **b)** Informar por escrito al **"PROVEEDOR"**, cualquier circunstancia particular, problema o requerimiento en la prestación del servicio, para que el mismo sea atendido o subsanado a la brevedad.
- **c)** Recibir los documentos y tramitar en tiempo y forma el pago correspondiente.
- **d)** En caso de ser procedente, emitir el oficio de entera satisfacción.
- **e)** Solicitar al momento del pago la aplicación de las penalizaciones señaladas en la cláusula **NOVENA** del presente contrato.
- **f)** Informar de manera oportuna a la Dirección General de Abastecimientos de la **"SECRETARÍA"** respecto del incumplimiento en la prestación del servicio materia del presente contrato, acompañando copia certificada u original del acta de hechos correspondiente.

El **"PROVEEDOR",** tendrá dentro de los alcances del presente contrato las siguientes obligaciones:

- **a)** Abastecer y/o prestar el servicio de conformidad con los términos y condiciones que se establecen en el presente contrato.
- **b)** Ser responsable del personal que realizara las labores y operaciones de lo adquirido materia del presente contrato.

JALISCO
GOBIERNO DEL ESTADO

Av. Fray Antonio Alcalde #1221,
Col. Miraflores, Guadalajara, Jalisco.
C.P. 44270 | 33 3818 2800

c) El personal de operación será responsabilidad directa de el **"PROVEEDOR"** por lo que exime a la **"SECRETARÍA"** de cualquier tipo de responsabilidad legal que se pudiera presentar antes, durante y después de la vigencia del presente contrato.
d) Proporcionar los elementos y materiales necesarios para la realización del objeto materia del presente contrato.
e) Supervisar el desarrollo de las actividades materia del presente contrato previo, durante y al finalizar de las mismas.
f) Aplicar al máximo su capacidad y conocimientos para cumplir satisfactoriamente con el objeto del presente instrumento.
g) Responder por falta de profesionalismo y en general cualquier incumplimiento a la prestación del servicio en los términos del presente contrato.
h) Salvaguardar el uso, la integridad, y confidencialidad de la información que se le proporcione, para su desarrollo del abastecimiento y/o prestación de lo adquirido.
i) Mantener constante comunicación con la dependencia designada como responsable por la **"SECRETARÍA"** para el seguimiento del presente contrato.

DÉCIMA PRIMERA.- ADMINISTRACIÓN, VERIFICACIÓN, SUPERVISIÓN Y ACEPTACIÓN DEL SERVICIO. La **"SECRETARÍA"** designa como responsable de administrar y vigilar el cumplimiento del presente contrato a la **Lic. Stephanie Viridiana Carrillo**, en su carácter de **Directora Administrativa**, con el objeto de verificar el óptimo cumplimiento del mismo, por lo que indicará al **"PROVEEDOR"** las observaciones que se estimen pertinentes, quedando éste obligado a corregir las anomalías que le sean indicadas, así como deficiencias en la prestación del servicio.

Las **"PARTES"** acuerdan que la **"SECRETARÍA"**, es la encargada de verificar que el servicio objeto de este contrato cumpla con las especificaciones acordadas por las **"PARTES"**, ya que es la receptora final del objeto de dicho instrumento.

Asimismo, la **"SECRETARÍA"** sólo aceptará el servicio de la póliza objeto del presente contrato y tramitará el pago del mismo previa verificación de las especificaciones requeridas, de conformidad con el presente contrato, así como la propuesta y el requerimiento asociado a ésta. La inspección del mismo consistirá en la verificación del cumplimiento de las especificaciones técnicas establecidas en el contrato, así como la propuesta y el requerimiento asociado a ésta.

En tal virtud, el **"PROVEEDOR"** manifiesta expresamente su conformidad de que hasta en tanto no se cumpla de conformidad con lo establecido en el párrafo anterior, el servicio, no se tendrá por aceptado por parte de la **"SECRETARÍA"**.

DÉCIMA SEGUNDA.- DE LA RESCISIÓN. De conformidad con lo dispuesto por el artículo 85 de la **"LEY"**, la **"SECRETARÍA"** podrá optar por el cumplimiento forzoso de este contrato o su rescisión, sin necesidad de declaración judicial alguna para que operen, siempre y cuando el **"PROVEEDOR"** incumpla con cualquier obligación establecida en las bases, el fallo de adjudicación y la propuesta aprobada, o en el presente contrato; o bien cuando el servicio de la póliza objeto de este contrato sea de características inferiores a las solicitadas en las bases en perjuicio de la **"SECRETARÍA"**. Este hecho será notificado de manera indubitable al **"PROVEEDOR"**. Se entenderá por incumplimiento, de manera enunciativa, más no limitativa, lo siguiente:

a) Si incurre en responsabilidad por errores u omisiones en su actuación;
b) Si incurre en negligencia en la prestación del servicio objeto del presente contrato, sin justificación para la **"SECRETARÍA"**;
c) Si transfiere en todo o en parte las obligaciones que deriven del presente contrato a un tercero ajeno a la relación contractual;
d) Si cede los derechos de cobro derivados del contrato, sin contar con la conformidad previa y por escrito de la **"SECRETARÍA"**;
e) Si suspende total o parcialmente y sin causa justificada la prestación del servicio de la póliza objeto del presente contrato o no les otorga la debida atención conforme a las instrucciones de la **"SECRETARÍA"**;
f) Si no presta el servicio en tiempo y forma conforme a lo establecido en el presente contrato, así como la propuesta y el requerimiento asociado a ésta;
g) Si no proporciona a la **"SECRETARÍA"** o a las dependencias que tengan facultades, los datos necesarios para la inspección, vigilancia y supervisión de la prestación del servicio de la póliza objeto del presente contrato;
h) Si cambia de nacionalidad e invoca la protección de su gobierno contra reclamaciones y órdenes de la **"SECRETARÍA"**;
i) Si es declarado en concurso mercantil por autoridad competente o por cualquier otra causa distinta o análoga que afecte su patrimonio;
j) Si no acepta pagar penalizaciones o no repara los daños o pérdidas, por argumentar que no le son directamente imputables, sino a uno de sus asociados o filiales o a cualquier otra causa que no sea de fuerza mayor o caso fortuito;

JALISCO
GOBIERNO DEL ESTADO
Av. Fray Antonio Alcalde #1221,
Col. Miraflores, Guadalajara, Jalisco.
C.P. 44270 | 33 3818 2800

k) Si el **"PROVEEDOR"** no presta el servicio de la póliza objeto de este contrato de acuerdo con las normas, la calidad, eficiencia y especificaciones requeridas por la **"SECRETARÍA"** conforme a las cláusulas del presente contrato, así como la propuesta y el requerimiento asociado a ésta;

l) Si divulga, transfiere o utiliza la información que conozca en el desarrollo del cumplimiento del objeto del presente contrato, sin contar con la autorización de la **"SECRETARÍA"** en los términos del presente instrumento jurídico;

m) Si se comprueba la falsedad de alguna manifestación contenida en el apartado de sus declaraciones del presente contrato;

n) Cuando el **"PROVEEDOR"** y/o su personal, impidan el desempeño normal de labores de la **"SECRETARÍA"**, durante la prestación del servicio, por causas distintas a la naturaleza del objeto del mismo;

o) Cuando exista conocimiento y se corrobore mediante resolución definitiva de autoridad competente que el **"PROVEEDOR"** incurrió en violaciones en materia penal, civil, fiscal, mercantil o administrativa que redunde en perjuicio de los intereses de la **"SECRETARÍA"** en cuanto al cumplimiento oportuno y eficaz en la prestación del servicio de la póliza objeto del presente contrato; y

p) En general, incurra en incumplimiento total o parcial de las obligaciones que se estipulen en el presente contrato o de las disposiciones de la **"LEY"** y su **"REGLAMENTO"**.

Para el caso de optar por la rescisión del contrato, la **"SECRETARÍA"** comunicará por escrito al **"PROVEEDOR"** el incumplimiento en que haya incurrido, para que en un término de 5 (cinco) días hábiles contados a partir de la notificación, exponga lo que a su derecho convenga y aporte en su caso las pruebas que estime pertinentes.

Transcurrido dicho término la **"SECRETARÍA"**, en un plazo de 15 (quince) días hábiles siguientes, tomando en consideración los argumentos y pruebas que hubiere hecho el **"PROVEEDOR"**, determinará de manera fundada y motivada dar o no por rescindido el contrato, y comunicará al **"PROVEEDOR"** dicha determinación dentro del citado plazo.

Cuando se rescinda el contrato, se formulará el finiquito correspondiente, a efecto de hacer constar los pagos que deba efectuar la **"SECRETARÍA"** por concepto del contrato hasta el momento de rescisión.

El **"PROVEEDOR"** se obliga a efectuar el pago del 10% de la cantidad señalada en la cláusula **CUARTA** de este Contrato, en caso de que la **"SECRETARÍA"** decida rescindir el presente contrato, por causas imputables al **"PROVEEDOR"**. De ser el caso, para efectos del presente párrafo, la **"SECRETARÍA"** podrá hacer efectiva la garantía señalada en la cláusula **SÉPTIMA** anterior, o en su caso podrá reclamar al **"PROVEEDOR"**, el pago directo de la cantidad a la que equivalga dicho porcentaje.

Las **"PARTES"** convienen que en caso de incumplimiento de las obligaciones a cargo del **"PROVEEDOR"**, la **"SECRETARÍA"** independientemente de las penas pactadas, podrá exigir el pago de daños y perjuicios de conformidad con el artículo 107 del **"REGLAMENTO"** de la **"LEY"**, además de poder solicitar el cumplimiento forzoso de este contrato o su rescisión.

Iniciado un procedimiento de conciliación, la **"SECRETARÍA"** podrá suspender el trámite del procedimiento de rescisión.

Si previamente a la determinación de dar por rescindido el contrato se prestara el servicio, el procedimiento iniciado quedará sin efecto, previa aceptación y verificación de la **"SECRETARÍA"** de que continúa vigente la necesidad del servicio, aplicando, en su caso, las penas convencionales correspondientes.

La **"SECRETARÍA"** podrá determinar no dar por rescindido el contrato, cuando durante el procedimiento advierta que la rescisión del mismo pudiera ocasionar algún daño o afectación a las funciones que tiene encomendadas. En este supuesto, la **"SECRETARÍA"** elaborará un dictamen en el cual justifique que los impactos económicos o de operación que se ocasionarían con la rescisión del contrato resultarían más inconvenientes.

Al no dar por rescindido el contrato, la **"SECRETARÍA"** establecerá con el **"PROVEEDOR"** otro plazo, que le permita subsanar el incumplimiento que hubiere motivado el inicio del procedimiento. El convenio modificatorio que al efecto se celebre deberá atender a las condiciones previstas por los dos últimos párrafos del artículo 80 de la **"LEY"**.

Cuando se presente cualquiera de los casos mencionados, la **"SECRETARÍA"** quedará expresamente facultada para optar por exigir el cumplimiento del contrato, aplicando las penas convencionales y/o rescindirlo, siendo esta situación una facultad potestativa.

Si se llevara a cabo la rescisión del contrato, y en el caso de que el **"PROVEEDOR"** se le hubieran entregado pagos progresivos, éste deberá de reintegrarlos más los intereses correspondientes.

JALISCO
GOBIERNO DEL ESTADO

Av. Fray Antonio Alcalde #1221,
Col. Miraflores, Guadalajara, Jalisco.
C.P. 44270 | 33 3818 2800

Los intereses se calcularán sobre el monto de los pagos progresivos efectuados y se computarán por días naturales desde la fecha de su entrega hasta la fecha en que se pongan efectivamente las cantidades a disposición de la **"SECRETARÍA"**.

El **"PROVEEDOR"** será responsable por los daños y perjuicios que le cause a la **"SECRETARÍA"**.

DÉCIMA TERCERA.- DEFECTOS Y VICIOS OCULTOS. El **"PROVEEDOR"** queda obligado ante la **"SECRETARÍA"** a responder de los defectos y vicios ocultos derivados de las obligaciones del presente contrato, así como de cualquier otra responsabilidad en que hubiere incurrido, en los términos señalados en este instrumento jurídico, así como la propuesta y el requerimiento asociado a ésta, y/o en la legislación aplicable en la materia.

Para los efectos de la presente cláusula, se entiende por vicios ocultos los defectos o falta de calidad en general, que existan en los servicios que preste el **"PROVEEDOR"**.

DÉCIMA CUARTA.- IMPUESTOS Y DERECHOS. Los impuestos, derechos y gastos que procedan con motivo de la prestación del servicio de la póliza, objeto del presente contrato, serán pagados por el **"PROVEEDOR"**, mismos que no serán repercutidos a la **"SECRETARÍA"**.

La **"SECRETARÍA"** sólo cubrirá, cuando aplique, lo correspondiente al IVA, en los términos de la normatividad aplicable y de conformidad con las disposiciones fiscales vigentes.

DÉCIMA QUINTA.- DEL RECHAZO. Las **"PARTES"** acuerdan que la **"SECRETARÍA"** no estará obligada a recibir o aprobar aquel servicio que el **"PROVEEDOR"** intente prestar, cuando a juicio de la **"SECRETARÍA"**, la característica del mismo difiera, o sea inferior de aquellas señaladas en el fallo de adjudicación y/o las bases, su junta aclaratoria, la propuesta aprobada, así como en el presente contrato. El rechazo del servicio deberá ser informado por la **"SECRETARÍA"** por escrito al **"PROVEEDOR"**. La falta de aceptación o aprobación del servicio con motivo de la presente cláusula, aun en casos en que ya haya sido prestado el servicio por parte del **"PROVEEDOR"**, no será motivo para considerar interrumpidos los plazos pactados para su prestación para efectos de las penas convencionales, e inclusive para la rescisión del presente contrato.

Cuando el servicio sea rechazado por la **"SECRETARÍA"** por resultar faltos de calidad en general o por ser de diferentes especificaciones a las solicitadas, y hubiesen sido pagados, el **"PROVEEDOR"** se obliga a devolver las cantidades pagadas con los intereses correspondientes, aplicando una tasa equivalente al interés legal sobre el monto a devolver, u obligarse el **"PROVEEDOR"** en este supuesto a prestarlos nuevamente bajo su exclusiva responsabilidad y sin costo adicional para la la **"SECRETARÍA"**.

DÉCIMA SEXTA.- LICENCIAS, AUTORIZACIONES Y PERMISOS. El **"PROVEEDOR"** será responsable de tramitar y contar con las licencias, autorizaciones y permisos que conforme a otras disposiciones sea necesario contar para la prestación del servicio correspondiente.

DÉCIMA SÉPTIMA.- RESPONSABILIDAD. El **"PROVEEDOR"** se obliga a responder por su cuenta y riesgo de los daños y/o perjuicios que por inobservancia o negligencia de su parte lleguen a causar a la **"SECRETARÍA"**, con motivo de las obligaciones pactadas, o bien por los defectos o vicios ocultos en el servicio prestado, de conformidad con lo establecido en el artículo 86 de la **"LEY"**.

DÉCIMA OCTAVA.- DE LA CESIÓN. El **"PROVEEDOR"** se obliga a no ceder a terceras personas físicas o morales los derechos y obligaciones derivados de este contrato y sus anexos. Sin embargo, podrá ceder los derechos de cobro, siempre y cuando cuente con el consentimiento previo y expreso de la **"SECRETARÍA"** para tal fin, de conformidad al artículo 77 punto 5, de la **"LEY"**.

DÉCIMA NOVENA.- DE LAS RELACIONES LABORALES. Las **"PARTES"** manifiestan expresamente que la relación que se deriva del presente contrato, no crea respecto de una y otra relación alguna de patrón, mandatario, subordinado, dependiente o empleado. En tal razón, el **"PROVEEDOR"** será responsable por la o las personas que contrate o emplee para cumplir con las obligaciones adquiridas mediante este contrato, obligándose a responder y sacar a salvo a la **"SECRETARÍA"** de cualquier acción o derecho que indistintamente se les reclame con motivo de prestaciones contenidas en la legislación en materia laboral, de seguridad social, fiscal, civil, penal o cualquier otra, en el entendido de que lo señalado con anterioridad queda subsistente por el periodo que la legislación aplicable señale, y no por el periodo que duren vigentes este contrato o sus garantías.

VIGÉSIMA.- DE LA PROPIEDAD INDUSTRIAL Y DERECHOS DE AUTOR. El **"PROVEEDOR"** asumirá la responsabilidad total para el caso de que se infrinjan derechos inherentes a la propiedad intelectual, patentes, marcas o cualquier otro derecho de tercero, con motivo de la prestación del servicio de la póliza materia del presente contrato, o de la firma de este documento, liberando a la **"SECRETARÍA"** de cualquier responsabilidad industrial o derechos de autor que puedan relacionarse con este instrumento, obligándose a salir en su defensa si por cualquier motivo, llegare a ser reclamado por estos y además, a pagar, sin derecho a réplica contra él, cualquier

JALISCO
GOBIERNO DEL ESTADO

Av. Fray Antonio Alcalde #1221,
Col. Miraflores, Guadalajara, Jalisco.
C.P. 44270 | 33 3818 2800

cantidad o prestación a que pueda ser condenado por autoridad competente con la Ley Federal de Protección a la Propiedad Industrial y la Ley Federal del Derecho de Autor.

VIGÉSIMA PRIMERA.- MODIFICACIONES DEL CONTRATO. Las **"PARTES"** están de acuerdo en que por necesidades de la **"SECRETARÍA"** por razones justificadas y explicitas, dentro del presupuesto aprobado y/o disponible podrá incrementar el monto total del contrato o cantidad de servicios objeto del presente contrato, de conformidad con el artículo 80 de la **"LEY"**, siempre y cuando las modificaciones no rebasen en su conjunto el 20% (veinte por ciento) del monto o cantidad establecidos originalmente. Lo anterior, se formalizará mediante la celebración de una adenda al Contrato Principal. Asimismo, con fundamento en el artículo 103 del **"REGLAMENTO"**, el **"PROVEEDOR"** deberá entregar las modificaciones respectivas de las garantías, señaladas en la cláusula **SÉPTIMA** de este contrato.

Por caso fortuito o de fuerza mayor, o por causas atribuibles a la **"DEPENDENCIA"**, le fuera imposible a el **"PROVEEDOR"** cumplir con sus obligaciones contratadas, solicitará oportunamente y por escrito a la **"SECRETARIA"**, la ampliación del término para su cumplimiento, según lo considere necesario, expresando los motivos en que apoye su solicitud, quien resolverá en un plazo no mayor a 08 días naturales, sobre la procedencia de la prórroga.

Tratándose de causas imputables a la **"SECRETARÍA"**, no se requerirá de la solicitud del **"PROVEEDOR".**

Al presentarse caso fortuito, fuerza mayor o emergencia declarada por autoridad competente, la **"SECRETARÍA"** no será responsable en la continuación con las obligaciones contractuales, salvo la obligación del pago de los bienes abastecidos o servicios prestados, hasta antes de presentarse la circunstancia, lo que se notificara por escrito a el **"PROVEEDOR",** especificando los detalles de la existencia de dicha condición, pudiendo en todo caso la **"SECRETARÍA"** acordar el cumplimiento total o parcial del objeto del contrato.

VIGÉSIMA SEGUNDA.- DE LA TERMINACIÓN ANTICIPADA. De conformidad con el artículo 89 de la **"LEY"**, la **"SECRETARÍA"** podrá dar por terminado el presente contrato en cualquier momento sin responsabilidad para sí, cuando se extinga la necesidad de contar con el servicio de la póliza objeto del presente contrato, por tratarse de causas de interés general o público, por cambios en el proyecto o programa para los cuales se haya pretendido destinar el objeto de este contrato, cuando se corra el riesgo de ocasionar algún daño o perjuicio a la **"SECRETARÍA"** o cualquier Dependencia o Entidad del Poder Ejecutivo del Estado, o por caso fortuito o fuerza mayor, bastando únicamente la notificación que se realice al **"PROVEEDOR"** para que dicha terminación pueda surtir efectos; o bien por acuerdo entre las **"PARTES"**. En cualquier caso, se realizará el pago de los gastos generados al **"PROVEEDOR"** hasta el momento que se notifique la terminación, siempre y cuando dichos gastos estén debidamente comprobados por el **"PROVEEDOR"**.

VIGÉSIMA TERCERA.- DE LAS NOTIFICACIONES. La comunicación entre las **"PARTES"** será por escrito y notificadas en los domicilios plasmados en este contrato constatando de forma fehaciente e indubitable constar su notificación.

VIGÉSIMA CUARTA.- DE LA AUTORIZACIÓN PARA UTILIZAR DATOS PERSONALES. El **"PROVEEDOR"** manifiesta tener conocimiento de que la **"SECRETARÍA"** y en general las dependencias y entidades del Poder Ejecutivo del Estado de Jalisco, están sujetos a las disposiciones contenidas en la legislación en materia de acceso a la información pública gubernamental, y que cuentan con diversas obligaciones, entre las que destacan la publicación de convenios, contratos y demás instrumentos jurídicos que celebren. En este contexto, el **"PROVEEDOR"** manifiesta su consentimiento expreso para que al presente contrato se le dé la publicidad que la legislación invocada disponga, en las formas que la misma determine.

Las **"PARTES"** se comprometen a salvaguardar el uso, la integridad y confidencialidad de la información que se les proporcione, así mismo no podrán ostentar poder alguno de decisión sobre el alcance y contenidos de los mismos. De igual manera, los datos confidenciales o sensibles que le sean trasladados no podrán ser utilizados para fines distintos a los establecidos, debiendo implementar medidas de seguridad adecuadas, tanto físicas, técnicas y administrativas, mediante el ejercicio de los servicios adquiridos, de conformidad a lo establecido en los artículos 65 y 75 numeral 1, fracción II, de la Ley de Protección de Datos Personales en posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

VIGÉSIMA QUINTA.- DE LA COMPETENCIA Y JURISDICCIÓN. Para la interpretación y cumplimiento del presente contrato, así como para resolver todo aquello que no esté previamente estipulado en él, las **"PARTES"** acuerdan en regirse en primer término por lo dispuesto en el fallo de adjudicación y/o las bases y su junta aclaratoria, y para lo no previsto en ellas, se sujetarán a la legislación aplicable en el Estado de Jalisco, sometiéndose expresamente a la jurisdicción de los Tribunales estatales o federales, que se encuentran en la circunscripción territorial del Primer Partido Judicial del Estado de Jalisco, renunciando al fuero que por razón de su domicilio presente o futuro les pudiera corresponder.

JALISCO
GOBIERNO DEL ESTADO

Av. Fray Antonio Alcalde #1221,
Col. Miraflores, Guadalajara, Jalisco.
C.P. 44270 | 33 3818 2800

VIGÉSIMA SEXTA.- Ambas **"PARTES"** manifiestan que el presente acto jurídico lo celebran sin coacción, dolo, violencia, lesión o mala fe que pudiera afectar de nulidad la voluntad de las **"PARTES"**.

Leído que fue el presente contrato por las **"PARTES"** y enteradas de su alcance y contenido, lo firman éstas de común acuerdo en 5 cinco tantos, el **día 20 del mes de Julio del año 2026**, en la ciudad de Guadalajara, Jalisco.

LA "SECRETARÍA"	
Por Acuerdo Delegatorio **SECADMON/ACU/01/2026.**	
Lic. Jesús Ezequiel Martínez Nieto, **Director Ejecutivo y Padrón de Proveedores de la Secretaría de Administración del Poder Ejecutivo del Estado de Jalisco.**	Stephanie Viridiana Carrillo, **Directora Administrativa de la Secretaría de Administración del Poder Ejecutivo del Estado de Jalisco.**

EL "PROVEEDOR"
C. Ariel Cárdenas Peña, **Presidente del Consejo de Administración de BEEHIVE SYSTEMS, S.A. DE C.V.**

TESTIGO	**TESTIGO**
Ángel Eduardo Márquez Castellón, **Director de Fallos y Adjudicaciones de la Secretaría de Administración del Poder Ejecutivo del Estado de Jalisco.**	Mtra. Irma Guadalupe Márquez Sevilla, **Directora de lo Consultivo de la Secretaría de Administración del Poder Ejecutivo del Estado de Jalisco.**

EIGE/JFSR

LA PRESENTE HOJA CORRESPONDE AL CONTRATO NÚMERO **CTO-323/26**, CELEBRADO ENTRE LA **SECRETARÍA DE ADMINISTRACIÓN** DEL PODER EJECUTIVO DEL ESTADO DE JALISCO Y **BEEHIVE SYSTEMS, S.A. DE C.V.**

1.- ELIMINADO el número de identificación oficial, por ser un dato personal identificativo de conformidad con los artículos 21.1 fracción I y 3.2 fracción II inciso "a" de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, 3.1 fracción IX y X de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados en el Estado de Jalisco y sus Municipios.

JALISCO
GOBIERNO DEL ESTADO

Av. Fray Antonio Alcalde #1221,
Col. Miraflores, Guadalajara, Jalisco.
C.P. 44270 | 33 3818 2800

ANEXO ÚNICO

Contrato número CTO-323/26, de la Licitación Pública Local LPL 334/2026, "*PÓLIZA DE DESARROLLO, MANTENIMIENTO Y SOPORTE A LOS SISTEMAS Y PROCESOS INFORMÁTICOS CON FÁBRICA DE SOFTWARE*".

Contiene:

- **Propuesta Técnica del Proveedor.**

PROPUESTA TÉCNICA

Guadalajara, Jalisco a 15 de junio de 2026

SECRETARÍA DE ADMINISTRACIÓN
DEL GOBIERNO DEL ESTADO DE JALISCO
PRESENTE.

AT'N: Dirección General de Abastecimientos

Partida	Descripción	Unidad de Medida	Cantidad
1	Póliza de Desarrollo, Mantenimiento y Soporte a los Sistemas y Procesos Informáticos con Fábrica de Software.	Servicio	1

Tiempo de entrega: A partir del día del fallo y durante 12 meses.
Garantía: 12 meses a partir del fallo de la licitación, en servicios, licencias y mano de obra.

Requerimientos técnicos:
Partida 1. Póliza de Desarrollo, Mantenimiento y Soporte a los Sistemas y Procesos Informáticos con Fábrica de Software

5.1. ALCANCE DEL REQUERIMIENTO Y DISPOSICIÓN DEL PERSONAL.

Los requerimientos se darán a conocer a **BEEHIVE SYSTEMS S.A. DE C.V.** durante la vigencia de la póliza, para que la FSW intervenga en el desarrollo, mantenimiento o soporte según sea el caso.

5.1.1. LUGAR DE TRABAJO

BEEHIVE SYSTEMS S.A. DE C.V. se compromete a realizar las actividades relacionadas con el servicio objeto de esta propuesta técnica, en instalaciones propias de **BEEHIVE SYSTEMS S.A. DE C.V.** ya sea de manera física o remota, cumpliendo siempre con los objetivos y alcances de la presente propuesta técnica; no obstante, la convocante puede solicitar de manera expresa que para casos específicos **BEEHIVE SYSTEMS S.A. DE C.V.** desempeñe sus funciones en instalaciones propias de las diferentes dependencias y entidades del Gobierno del Estado de Jalisco. En dado caso de que **BEEHIVE SYSTEMS S.A. DE C.V.** se instale en las diferentes Dependencias o Entidades del Estado, nos comprometemos a proveer la infraestructura que sea necesaria para el desarrollo de nuestro trabajo. La convocante solo proporcionará el espacio físico para ello. Para el caso de las reuniones de trabajo, estas se podrán realizar de manera remota o presencial según lo requiera la DIG de la DGITG.

5.1.2. ESQUEMA DE TRABAJO

BEEHIVESYSTEMS
UNIFYING THE MANAGEMENT & SECURITY

El horario de trabajo del personal de **BEEHIVE SYSTEMS S.A. DE C.V.** será abierto de 7 días por 24 horas durante la vigencia del contrato, así como en los periodos de garantía para cada una de las soluciones tecnológicas desarrolladas.

5.1.3. EVENTUALIDADES EXTRAORDINARIAS

Ante eventualidades no planeadas, la DGITG podrá coadyuvar con **BEEHIVE SYSTEMS S.A. DE C.V.** para brindar soluciones tecnológicas que permitirán mitigar y solucionar las eventualidades que se pudieran presentar durante la vigencia del contrato. Por tal motivo, la DIG de la DGITG tendrá la facultad de solicitar a **BEEHIVE SYSTEMS S.A. DE C.V.** que designe el personal necesario y/o asignar tareas directamente al personal de FSW que este trabajando en diferentes proyectos para el Gobierno del Estado de Jalisco de manera inmediata para apoyar en los proyectos que se requieran para mitigar las eventualidades.

5.1.4. BOLSA DE HORAS DE TRABAJO

Con el fin de que en **BEEHIVE SYSTEMS S.A. DE C.V.** tengamos las referencias que nos permitan establecer los recursos necesarios para elaborar nuestra propuesta, se listan de manera enunciativa más no limitativa distintos puntos destinados a la ejecución de todos los requerimientos descritos en el Anexo Técnico, tales como:

- MANTENIMIENTO Y SOPORTE A LA ARQUITECTURA BASE PARA DESARROLLO DE SISTEMAS Y APLICACIONES GUBERNAMENTALES
- DESARROLLO DE SOFTWARE
- SEGURIDAD DEL CÓDIGO
- OTROS SERVICIOS

BEEHIVE SYSTEMS S.A. DE C.V. se compromete a ejecutar todo lo anterior haciendo uso de una bolsa de hasta 78,300 horas, las cuales serán efectivas a partir del fallo y durante 12 meses.
Los puntos y cantidad de horas descritos anteriormente se proporcionan como una referencia con el fin de que **BEEHIVE SYSTEMS S.A. DE C.V.** pueda realizar su estimación de recursos necesarios y de costo. La cantidad de horas y servicios requeridos puede modificarse en función de los requerimientos de las distintas áreas del Gobierno del Estado de Jalisco.

5.1.5. ESTIMACIÓN DE HORAS

La estimación de horas de los requerimientos se realizará por medio de la técnica Delphi, como un mecanismo estructurado de consulta iterativa entre expertos, orientado a la obtención de consensos técnicos fundamentados.

Para la estimación, se considera que la unidad para determinar el costo de los servicios se denominará en horas de trabajo. La estimación se realizará a partir del siguiente flujo:

https://beehivesystems.mx contacto@beehivesystems.mx 33 1588 4412 / 33 8526 3103

BEEHIVESYSTEMS
UNIFYING THE MANAGEMENT & SECURITY

- Primero, se identificará quién será considerado como experto para emitir una estimación de horas, tanto del equipo de **BEEHIVE SYSTEMS S.A. DE C.V.** como del personal de la DIG de la DGITG y la DS de la DGTI que participarán en el proyecto que se requiere estimar.

  Para efectos del presente proceso, se entenderá como "expertos" a los perfiles con conocimiento técnico, funcional y/o de implementación directamente relacionado con el alcance del proyecto. La participación de dichos expertos será de carácter individual y técnico, sin que ello implique la conformación de un órgano colegiado formal.

- Se pondrá a disposición de todos los involucrados en el proceso de estimación la información que indique la DIG de la DGITG sobre el proyecto a estimar; en caso de que la información no sea suficiente para realizar la estimación por parte de los involucrados, **BEEHIVE SYSTEMS S.A. DE C.V.** realizará las actividades y trabajos que le requiera la DIG de la DGITG a fin de obtener más información que permita realizar dicha estimación.
  Adicionalmente, toda la información compartida quedará documentada y accesible para los expertos participantes, a fin de garantizar trazabilidad y sustento en las estimaciones emitidas.

- Si la estimación de todos los involucrados en el proceso es igual o menor al 20% respecto al promedio, entonces el costo del servicio será determinado por el promedio de las estimaciones, asentando un riesgo de que el esfuerzo puede incrementarse siempre y cuando este incremento sea avalado por la DIG de la DGITG. En caso de que las estimaciones de los expertos involucrados en el proyecto presenten variaciones mayores al 20%, se revisará toda la información y proyecciones realizadas. La revisión la realizará el equipo de la DIG de la DGITG, quien solicitará a los expertos reconsiderar sus estimaciones tomando en cuenta las observaciones técnicas emitidas, pudiendo llevarse a cabo iteraciones adicionales del ejercicio Delphi hasta reducir la dispersión y lograr un nivel razonable de convergencia.

  El consenso se entenderá alcanzado cuando las estimaciones se encuentren dentro del rango de variación permitido o cuando, derivado de las iteraciones realizadas, exista alineación técnica suficiente entre los expertos respecto al esfuerzo requerido. Este consenso no implicará votación ni la formalización de sesiones colegiadas, sino la convergencia documentada de opiniones técnicas independientes.

5.2. MANTENIMIENTO Y SOPORTE A LA ARQUITECTURA BASE PARA DESARROLLO DE SISTEMAS Y APLICACIONES GUBERNAMENTALES

BEEHIVE SYSTEMS S.A. DE C.V. se compromete a entregar servicios de mantenimiento y soporte a la arquitectura base para desarrollo de sistemas y aplicaciones gubernamentales, la cual cuenta con características tales como capacidad de trabajar local, nube e híbrido, alta disponibilidad, escalabilidad, entre otras. Esta arquitectura base incluye, de manera enunciativa mas no limitativa los puntos siguientes:

5.2.1. ARQUITECTURA DE COMPONENTES TECNOLÓGICOS

https://beehivesystems.mx contacto@beehivesystems.mx 33 1588 4412 / 33 8526 3103

BEEHIVESYSTEMS
UNIFYING THE MANAGEMENT & SECURITY

Los componentes tecnológicos se refieren a los elementos o tecnologías generales que son susceptibles de requerirse en el desarrollo de sistemas o aplicaciones gubernamentales y pueden ser componentes de la arquitectura. Los requerimientos de los componentes tecnológicos de referencia que se listan enseguida:

- Documentación
  - En caso de requerirse, se utilizarán herramientas que permitan la documentación y pruebas de API's RestFul
- Telemetría y monitoreo
  - En caso de requerirse, se obtendrá la trazabilidad en múltiples sistemas que permitan monitorear y depurar transacciones en aplicaciones y microservicios
  - En caso de requerirse, se realizará el monitoreo a los sistemas, que entregan métricas y alertas, desde infraestructura hasta aplicaciones y microservicios
- Aplicaciones móviles y web (Front, Back y APIS)
  - Aplicaciones web
    - Backend
      - Los framework o tecnologías serán modulares.
      - Se permitirá la fácil creación de API Restful.
      - En caso de ser necesario, se reducirá la propensión a errores de programación.
      - En caso de requerirse, se realizarán conexiones homologadas a la base de datos por medio de modelos ORM.
    - Frontend
      - Los framework o tecnologías permitirán que la arquitectura sea robusta y dinámica.
      - Se permitirá el manejo de componentes, rutas y servicios.
      - En caso de requerirse, se reducirá la propensión a errores de programación.
  - Aplicaciones móviles
    - Backend
      - Los framework o tecnologías serán modulares.
      - Se permitirá la fácil creación de API Restful.
      - En caso de ser necesario, se reducirá la propensión a errores de programación.
      - En caso de requerirse, se realizarán conexiones homologadas a la base de datos por medio de modelos ORM.
    - Frontend
      - Se contará con la capacidad de generación de aplicación para Android o iOS.
      - En caso de ser necesario, se reducirá la propensión a errores de programación.
      - En caso de ser necesario, se contará con la capacidad de integrarse con funcionalidades nativas de Android o iOS.
      - En caso de ser necesario, se realizarán integraciones con frameworks.
- Base de datos
  - En caso de ser necesario, se soportarán implementaciones.

https://beehivesystems.mx contacto@beehivesystems.mx 33 1588 4412 / 33 8526 3103

- Monolíticas.
- Distribuidas.
- Compartidas.

- En caso de ser necesario, se contará con la capacidad de realizar consultas a gran cantidad de datos.
- En caso de ser necesario, se permitirá la integración con sistemas de reporteo BI y ETL.

- Cache y colas
  - **BEEHIVE SYSTEMS S.A. DE C.V.** propone un servicio eficiente de alta velocidad y baja latencia.
  - En caso de ser necesario, se gestionarán flujos y colas en sistemas distribuidos.
  - En caso de ser necesario, se contará con soporte de procesamiento concurrente de alto desempeño y disponibilidad.
- Inteligencia artificial y machine learning
  - En caso de ser necesario, se implementarán herramientas y metodologías que faciliten la gestión del ciclo de vida de los modelos de IA, asegurando su correcto desarrollo, monitoreo y despliegue en producción.
  - En caso de ser necesario, la arquitectura permitirá la escalabilidad y trazabilidad de los modelos, con procesos adecuados para la detección y mitigación de sesgos en los datos utilizados.
  - En caso de ser necesario, se implementarán mecanismos de auditoría y gobernanza en los modelos para garantizar la seguridad y cumplimiento normativo.
  - En caso de ser necesario, se incluirán procesos automatizados para el entrenamiento, validación y versionamiento de modelos de Machine Learning.
  - Para la implementación de modelos de IA, **BEEHIVE SYSTEMS S.A. DE C.V.** propone utilizar plataformas y herramientas especializadas en la gestión integral del ciclo de vida de los modelos facilitando su desarrollo, despliegue y monitoreo.
  - **BEEHIVE SYSTEMS S.A. DE C.V.** propone aplicar buenas prácticas a través de técnicas de explicabilidad y detección de sesgos, utilizando herramientas especializadas en la interpretación de modelos de inteligencia artificial.
  - En caso de ser necesario, la observabilidad y monitoreo de modelos en producción se realizará mediante herramientas especializadas que permiten supervisar métricas clave y detectar anomalías en su desempeño.
  - **BEEHIVE SYSTEMS S.A. DE C.V.** propone el uso de herramientas especializadas para la visualización y análisis en tiempo real.
- Fuentes de datos y versionamiento
  - **BEEHIVE SYSTEMS S.A. DE C.V.** propone el uso de diversas plataformas para el almacenamiento y gestión de datos estructurados y no estructurados.
  - **BEEHIVE SYSTEMS S.A. DE C.V.** propone implementar un sistema de control de versiones de datos para garantizar reproducibilidad en modelos de IA.
- Procesamiento y orquestación de datos
  - **BEEHIVE SYSTEMS S.A. DE C.V.** propone utilizar herramientas para el procesamiento masivo de datos en entornos distribuidos, mejorando el rendimiento y la escalabilidad.
  - **BEEHIVE SYSTEMS S.A. DE C.V.** propone utilizar herramientas especializadas para la orquestación de procesos de ETL y la automatización de flujos de datos.
- Machine Learning (ML)

  - **BEEHIVE SYSTEMS S.A. DE C.V.** propone el uso de herramientas especializadas para la experimentación y gestión de modelos de machine learning.
  - **BEEHIVE SYSTEMS S.A. DE C.V.** propone utilizar herramientas especializadas para versionar modelos y registrar experimentos, asegurando la trazabilidad de resultados.
- Modelos de IA/ML y su implementación
  - **BEEHIVE SYSTEMS S.A. DE C.V.** propone utilizar bibliotecas especializadas en Deep Learning para la experimentación y entrenamiento de modelos.
  - **BEEHIVE SYSTEMS S.A. DE C.V.** propone integrar modelos de lenguaje a gran escala dentro de la arquitectura para diversas aplicaciones.
- Publicación y monitoreo de modelos
  - **BEEHIVE SYSTEMS S.A. DE C.V.** propone utilizar herramientas especializadas para la publicación y suscripción a eventos generados por modelos en producción.
  - **BEEHIVE SYSTEMS S.A. DE C.V.** propone implementar soluciones especializadas para la persistencia de métricas, facilitando el monitoreo y la observabilidad de modelos.
  - **BEEHIVE SYSTEMS S.A. DE C.V.** propone utilizar herramientas especializadas para la visualización de indicadores clave y métricas de rendimiento de modelos.
- Blockchain
  - En caso de ser necesario, se implementarán tecnologías de blockchain para garantizar la trazabilidad, seguridad y automatización de procesos críticos dentro de la arquitectura tecnológica.
  - **BEEHIVE SYSTEMS S.A. DE C.V.** propone la adopción de contratos inteligentes para la automatización de flujos de trabajo, asegurando la integridad y verificabilidad de la información.
  - En caso de ser necesario, se **BEEHIVE SYSTEMS S.A. DE C.V.** propone establecer mecanismos de validación y pruebas de contratos inteligentes antes de su despliegue, utilizando herramientas especializadas para su verificación y simulación.
  - En caso de ser necesario, se implementarán procesos de monitoreo de la actividad en la red blockchain mediante herramientas especializadas para la observabilidad y supervisión.
  - Para el almacenamiento de datos complementarios de la blockchain, **BEEHIVE SYSTEMS S.A. DE C.V.** propone el uso de bases de datos híbridas que permitan un acceso eficiente a la información sin comprometer la descentralización.
  - En caso de ser necesario, **BEEHIVE SYSTEMS S.A. DE C.V.** propone establecer un modelo de seguridad y gobernanza de contratos inteligentes mediante protocolos de auditoría y gestión de acceso.
- Base de datos distribuida y almacenamiento de información
  - **BEEHIVE SYSTEMS S.A. DE C.V.** propone utilizar bases de datos híbridas para almacenar transacciones y datos complementarios de blockchain.
  - **BEEHIVE SYSTEMS S.A. DE C.V.** propone utilizar soluciones especializadas para la gestión de archivos relacionados con transacciones y contratos inteligentes.
- Orquestación de contratos inteligentes
  - **BEEHIVE SYSTEMS S.A. DE C.V.** propone utilizar herramientas especializadas para la automatización y orquestación de contratos inteligentes.
  - **BEEHIVE SYSTEMS S.A. DE C.V.** propone utilizar herramientas especializadas para habilitar la comunicación asíncrona entre los nodos de la red blockchain.

- Monitoreo y seguridad de la red blockchain
  - **BEEHIVE SYSTEMS S.A. DE C.V.** propone utilizar herramientas especializadas para rastrear transacciones y detectar posibles anomalías en la blockchain.
  - **BEEHIVE SYSTEMS S.A. DE C.V.** propone utilizar herramientas especializadas para la creación de tableros visuales con información sobre la actividad en la red blockchain.
- Orquestación
  - En caso de ser necesario, se permitirá la orquestación de servicios distribuidos para la automatización, despliegue, escalado y manejo de aplicaciones.
  - En caso de ser necesario, se crearán, distribuirán y ejecutarán aplicaciones, garantizando portabilidad y consistencia.
  - En caso de ser necesario, se implementará una malla de servicios que facilite la comunicación, seguridad y monitoreo entre microservicios.
- Infraestructura
  - **BEEHIVE SYSTEMS S.A. DE C.V.** propone considerar la portabilidad de aplicaciones y microservicios.
  - En caso de ser necesario, se reducirán las diferencias de ambientes de producción, pruebas y desarrollo.
  - **BEEHIVE SYSTEMS S.A. DE C.V.** propone considerar la agilidad en el aprovisionamiento de recursos para el despliegue de aplicaciones.
  - **BEEHIVE SYSTEMS S.A. DE C.V.** propone considerar la implementación de aislamiento y seguridad entre aplicaciones.
  - **BEEHIVE SYSTEMS S.A. DE C.V.** propone considerar la integración con herramientas de CI y CD.
  - **BEEHIVE SYSTEMS S.A. DE C.V.** propone considerar el uso de herramientas que permitirán organizar, gestionar y coordinar aplicaciones distribuidas de manera eficiente.
  - **BEEHIVE SYSTEMS S.A. DE C.V.** propone considerar alta disponibilidad.
  - **BEEHIVE SYSTEMS S.A. DE C.V.** propone considerar balanceo de carga de trabajo adaptándose de manera automática.
  - **BEEHIVE SYSTEMS S.A. DE C.V.** propone considerar capacidad de balancear carga entre ambiente on-premise y ambientes en la nube.
  - **BEEHIVE SYSTEMS S.A. DE C.V.** propone gestionar el tráfico entre servicios, incluyendo el enrutamiento avanzado y balanceo de carga, failovers y políticas de circuit breaking.
  - **BEEHIVE SYSTEMS S.A. DE C.V.** propone considerar la tolerancia a fallos.
- Librerías auxiliares
  - **BEEHIVE SYSTEMS S.A. DE C.V.** propone reducir la propensión a errores de programación.
  - En caso de ser necesario, se permitirá la creación de hojas de estilo de una manera organizada y eficiente con características avanzadas de CSS.
  - **BEEHIVE SYSTEMS S.A. DE C.V.** propone la compilación y empaquetado de recursos en un solo archivo.

En caso de que **BEEHIVE SYSTEMS S.A. DE C.V.** se adjudicado, se llevará a cabo una reunión entre la convocante y **BEEHIVE SYSTEMS S.A. DE C.V.** para gestionar la documentación, accesos y recursos necesarios para que **BEEHIVE SYSTEMS S.A. DE C.V.** comience a brindar los servicios de mantenimiento y soporte a la arquitectura base para desarrollo de sistemas y aplicaciones gubernamentales conforme a

las necesidades y especificaciones que le determine la convocante. Con el objetivo de avalar que **BEEHIVE SYSTEMS S.A. DE C.V.** cuenta con las capacidades técnicas para realizar los servicios de MANTENIMIENTO Y SOPORTE A LA ARQUITECTURA BASE PARA DESARROLLO DE SISTEMAS Y APLICACIONES GUBERNAMENTALES requeridos, **BEEHIVE SYSTEMS S.A. DE C.V.** presenta como parte de nuestra propuesta un documento en el que describimos como integraremos una aplicación existente a la arquitectura para desarrollo de sistemas y aplicaciones gubernamentales. El documento incluye los puntos o elementos siguientes:

- Definición de CI/CD
- Definición Gitops
- Un diagrama de referencia explicando el flujo de integración de aplicaciones considerando al menos los siguientes componentes:
    - Un repositorio de aplicación que contenga:
        - Unidad de pruebas
        - Calidad del código
        - Generación de imágenes (proyecto)
    - Un repositorio de infraestructura que contenga:
        - Aplicación
        - Infraestructura
        - Cluster
    - Un cluster de kubernetes:
        - Un cluster de desarrollo
        - Un cluster de producción
    - Se sugiere el uso de la Flux para el manejo de las políticas de actualización de imágenes, se debe presentar en el diagrama como se realizaría esta acción a través de flux.
    - Explicación del flujo
- Descripción detallada del proceso de despliegue continuo.

DESCRIPCIÓN DE CÓMO INTEGRAR UNA APLICACIÓN EXISTENTE A LA ARQUITECTURA PARA DESARROLLO DE SISTEMAS Y APLICACIONES GUBERNAMENTALES

Definición de CI/CD

Integración Continua (CI)

La Integración Continua (CI) se basa en la integración frecuente de cambios de código en un repositorio común. Esto permite detectar y corregir errores de forma temprana, garantizando que el código siempre esté en un estado funcional.

Entrega Continua (CD)

La Entrega Continua (CD) extiende este enfoque, automatizando el proceso de prueba y lanzamiento del software a entornos de pruebas o producción.

Definición Gitops

Se basa en el principio de que todo el estado del sistema (incluyendo la infraestructura) se gestiona a través de un repositorio Git.

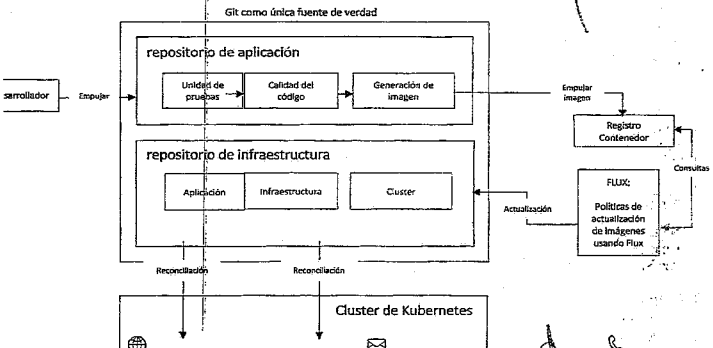
Enfoque:

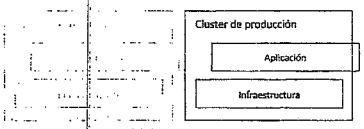
Infraestructura como código (IaC): La infraestructura no se configura directamente a través de interfaces gráficas o comandos manuales, se configura mediante los archivos de configuración del sistema directamente en un repositorio de código.

Procesos automatizados: Los cambios se implementan mediante pull requests, que son revisados y aprobados y luego se aplican automáticamente al entorno de destino.
Fuente de verdad: Git es el único "source of truth" (fuente de verdad) para la configuración de infraestructura.

Un diagrama de referencia explicando el flujo de integración de aplicaciones considerando al menos los siguientes componentes:

- Un repositorio de aplicación que contenga:
    - Unidad de pruebas
    - Calidad del código
    - Generación de imágenes (proyecto)
- Un repositorio de infraestructura que contenga:
    - Aplicación
    - Infraestructura
    - Cluster
- Un cluster de kubernetes:
    - Un cluster de producción
- Se sugiere el uso de la Flux para el manejo de las políticas de actualización de imágenes, se debe presentar en el diagrama como se realizaría esta acción a través de flux.





- Explicación del flujo

Un desarrollador realizará un push a un repositorio de código denominado repositorio de aplicación, este evento activará automáticamente los pipelines de CI/CD definidos en el repositorio, los cuales estarán estructurados en varias etapas con el objetivo de garantizar la calidad del código, la seguridad y la generación de imágenes de contenedor preparadas para el despliegue.

El pipeline de CI que se propone consta de las siguientes etapas:

Unidad de pruebas

Ejecutará pruebas unitarias específicas de la aplicación, asegurando que no haya regresiones ni errores en funcionalidades críticas, realizará un análisis estático del código para detectar problemas de estilo, sintaxis y buenas prácticas de programación relacionadas con las reglas de "linting" del proyecto.

Calidad del código

Verificará que el código cumpla con las normas de calidad definidas, garantizando mantenibilidad y legibilidad y detectará posibles vulnerabilidades de seguridad en el código fuente.

Generación de imagen

Generará una imagen de contenedor a partir del Dockerfile ubicado en la raíz del proyecto, la imagen se empujará al registro contenedor para su posterior uso en el despliegue.

Manejo de políticas de actualización de imágenes mediante Flux

Se definirá el despliegue de aplicaciones e infraestructura utilizando el enfoque GitOps, a través del framework Flux, este enfoque se implementará en un repositorio denominado repositorio de infraestructura, el cual contendrá la configuración necesaria para desplegar las aplicaciones en diferentes clusters. Dependiendo del tipo de cluster, se proponen las siguientes estrategias para el despliegue:

Clusters con Despliegue Automático

Se emplearán recursos como políticas de actualización de imágenes, el cual es un recurso personalizado de Flux que se usará para automatizar la actualización de contenedores en los archivos de Kubernetes basándose en una política específica para las imágenes de contenedor. También se emplearán recursos como ImageRepository, el cual es un recurso personalizado de Flux que define de qué registro de contenedores (como Docker Hub, GitLab Container Registry) se obtendrán las imágenes de contenedor y con qué frecuencia se revisará para monitorear cambios en el registro contenedor.
Al detectar una actualización en la imagen, se generará automáticamente una actualización en el repositorio de infraestructura sobre los tags de imágenes para actualizar el cluster sin necesidad de intervención manual.

Clusters sin Despliegue Automático

En estos entornos se requiere una acción manual para desplegar los cambios, proponen las siguientes opciones:

Opción 1: Uso de Tags e políticas de actualización de imágenes Personalizado

Una vez completadas las pruebas, se hará un push al repositorio "repositorio de aplicación" en una nueva rama que corresponde a una etiqueta (tag) de Git, esta etiqueta será utilizada para generar una imagen con el mismo tag, se utilizará políticas de actualización de imágenes distinto para esta rama, el cual se configurará en el repositorio de infraestructura y actualizará los entornos correspondientes.

Opción 2: Modificación Manual en repositorio de infraestructura

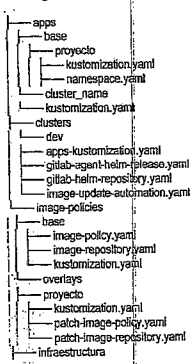
Se realizará una modificación manual en el repositorio de infraestructura para los tags de las imágenes a desplegar en una rama de desarrollo. Se creará un Merge Request (MR) hacia la rama main, al hacer el merge, los cambios se aplicarán al cluster y se desplegará la aplicación con las nuevas imágenes correspondientes.

Descripción detallada del proceso de despliegue continuo.

Toda la configuración de los proyectos para el proceso de despliegue continuo es utilizando kustomize para generar los build de archivos a utilizar por los clusters. **BEEHIVE SYSTEMS S.A. DE C.V.** propone que antes de editar los archivos de configuración en el repositorio de infraestructura, se revise como está

configurada la estructura de los diferentes componentes de infraestructura para la aplicación, para este proceso se propone el uso de kustomize, flux y generación de archivos yaml de kubernetes.

La estructura base del repositorio de infraestructura que se propone para el proceso de despliegue continuo es la siguiente:



apps/base: Se propone que contenga la configuración base de las aplicaciones que pueden ser utilizadas en multiples clusters

apps/cluster_name: Se propone que contenga aplicaciones que solo deban ejecutarse en el cluster con el nombre "cluster_name" y a demás contendrá overlays que sean necesarios para los proyectos base (ejemplo, agregar un prefijo al nombre de las aplicaciones, cambiar su namespace, cambiar la cantidad de replicas que debe levantar)

clusters: Se propone que contenga la configuración para cada uno de los clusters; dentro de cada cluster debe existir un apps-kustomization.yaml, el cual hará referencia a el kustomization.yaml que existe en apps/cluster_name y de ser necesaria realizará la actualización de imagenes un archivo de image-update-automation.yaml

image-policies: Se propone que contenga la configuración para automatización de image policy y sincronización del cluster o clusters, de momento, se hace referencia en /apps/cluster_name

infraestructura: Se propone que contenga la configuración de recursos de infraestructura que serán aplicados a todo el cluster para su funcionamiento, independiente a la configuración de aplicaciones.

5.3. DESARROLLO DE SOFTWARE

Los proyectos que forman parte de la Póliza de Desarrollo, Mantenimiento y Soporte a los Sistemas y Procesos Informáticos con Fábrica de Software serán informados a **BEEHIVE SYSTEMS S.A. DE C.V.** durante la vigencia de la póliza y conforme a las necesidades y requerimientos de las diferentes Dependencias y Entidades del Gobierno del Estado de Jalisco.

BEEHIVE SYSTEMS S.A. DE C.V. considera dentro del alcance de esta propuesta la ejecución de servicios de desarrollo de software para actividades de tipo:

- Nuevos proyectos.
- Migración de recursos y aplicaciones existentes.
- Otros servicios

En alcance a nuestra propuesta, **BEEHIVE SYSTEMS S.A. DE C.V.** considera las siguientes etapas, las cuales se tomarán de la bolsa de horas basada en las actividades descritas a continuación:

Captación:

Se describe a la fase de captación como el conjunto de actividades, servicios y recursos responsables de recibir, analizar, estimar y documentar los servicios de desarrollo de software solicitados por parte de las diversas Dependencias o Entidades del Gobierno del Estado de Jalisco. Como parte de los alcances de esta fase, **BEEHIVE SYSTEMS S.A. DE C.V.** será responsable de establecer una estructura organizacional que cubrirá roles funcionales tales como, arquitecto de software, administrador de proyectos, analista de negocios, líder técnico, dueño de producto, ingeniero de DevOps, así como otros perfiles que la DIG de la DGITG considere necesarios para cumplir de manera concreta y correcta con los servicios y entregables de la fase de captación.

Definición:

Se describe a la fase de definición como el conjunto de actividades, servicios y recursos responsables de definir, planear, priorizar, refinar, delimitar, asignar y documentar los requerimientos de los servicios de desarrollo de software solicitados por parte de las diversas Dependencias y Entidades del Gobierno del Estado de Jalisco. Como parte de los servicios de definición, **BEEHIVE SYSTEMS S.A. DE C.V.** será responsable de establecer una estructura organizacional que cubrirá roles funcionales tales como: arquitecto de software, administrador de proyectos, analista de negocios, líder técnico, dueño de producto, ingeniero de DevOps, desarrolladores de software especialistas en Front-End, desarrolladores de software especialistas en Back-End, desarrolladores de software Fullstack así como otros perfiles que la DIG de la DGITG considere necesarios para cumplir de manera concreta y correcta con los servicios y entregables de la fase de definición.

Desarrollo:

Se describe a la fase de desarrollo como el conjunto de actividades, servicios y recursos responsables de elaborar, revisar, implementar, desplegar, entregar y documentar el código necesario para cumplir con los requerimientos de los servicios de desarrollo de software solicitados por parte de las diversas Dependencias y Entidades del Gobierno del Estado de Jalisco. Como parte de los servicios de desarrollo, **BEEHIVE SYSTEMS S.A. DE C.V.** será responsable de establecer una estructura organizacional que cubra roles funcionales tales como: arquitecto de software, administrador de proyectos, líder técnico, dueño de producto, ingeniero de DevOps, desarrolladores de software especialistas en Front-End, desarrolladores de software especialistas en Back-End, desarrolladores de software Fullstack, analista

para el aseguramiento de la calidad, así como otros perfiles que la DIG de la DGITG considere necesarios para cumplir de manera concreta y correcta con los servicios y entregables de la fase de desarrollo.

Cierre:

Se describe a la fase de cierre como el conjunto de actividades, servicios y recursos necesarios para poder finalizar de manera formal y administrativa los trabajos relacionados con los servicios de desarrollo de software solicitados por parte de las diversas Dependencias y Entidades del Gobierno del Estado de Jalisco. Como parte de los servicios de cierre, **BEEHIVE SYSTEMS S.A. DE C.V.** se compromete a realizar las capacitaciones, despliegues, acompañamientos y otros servicios/actividades que se consideren necesarios para asegurar la correcta finalización de los servicios de desarrollo de software, para lo cual **BEEHIVE SYSTEMS S.A. DE C.V.** será responsable de establecer una estructura organizacional que cubra roles funcionales tales como: administrador de proyectos, líder técnico, dueño de producto, ingeniero de DevOps, analista para el aseguramiento de la calidad, así como otros perfiles que la DIG de la DGITG considere necesarios para cumplir de manera concreta y correcta con los servicios y entregables de la fase de cierre. En esta fase se realiza la cesión de derechos y se comparten los entregables (documentos) relacionados con los servicios. Es importante resaltar que los entregables deberán contar con la aprobación de la DIG de la DGITG para ser considerados como entregables correctos y finalizados.

Los productos derivados de los servicios de desarrollo de software se apegarán a los lineamientos de la arquitectura base para desarrollo de sistemas y aplicaciones gubernamentales; lo antes mencionado será avalado por la DIG de la DGITG. Con el objetivo de avalar que **BEEHIVE SYSTEMS S.A. DE C.V.** implementará procedimientos y mejores prácticas para el DESARROLLO DE SOFTWARE, presentamos como parte de nuestra propuesta un documento en el que describimos cómo realizaremos la gestión de los flujos de trabajo, con base en la estrategia de desarrollo Trunk-Based-Development. El documento incluye los puntos o elementos siguientes:

- Objetivo del proceso de trabajo
- Las herramientas que usan en su proceso de trabajo
- Roles de acuerdo con los señalados en este requerimiento
- Diagrama de proceso del flujo de trabajo considerando las siguientes etapas:
  - Captación
  - Definición
  - Desarrollo
  - Cierre
- Métricas de desempeño
- Objetivos de implementar Trunk-Based-Development
- Características del desarrollo basado en Trunk
- Flujo de trabajo enfocado al Desarrollo basado en Trunk

DESCRIPCIÓN DE GESTIÓN DE LOS FLUJOS DE TRABAJO CON BASE EN LA ESTRATEGIA DE DESARROLLO TRUNK-BASED-DEVELOPMENT

Objetivo del proceso de trabajo

Como objetivo se propone la estandarización del proceso de trabajo en bases de código compartidas para maximizar la eficiencia, reducir conflictos y asegurar la calidad, mientras se mantiene un proceso transparente de seguimiento para todos los involucrados.

Las herramientas que usan en su proceso de trabajo

Se propone una herramienta que funcione como Service Desk: Herramienta para la captación, definición y seguimiento de solicitudes de los usuarios finales que permitirá aplicar actualizaciones y / o nuevas funcionalidades a los productos que se desarrollarán.

Se propone una herramienta de administración Software: Herramienta central que será utilizada en la planificación de requerimientos, tareas a realizar e implementaciones de funcionalidades de software por los equipos autónomos de desarrollo.

Roles de acuerdo con los señalados en este requerimiento

De manera enunciativa mas no limitativa **BEEHIVE SYSTEMS S.A. DE C.V.** propone los siguientes roles:

Dueño de producto:
- Revisará y organizará el backlog.
- Asegurará que los criterios de aceptación estén claros.
- Mediará entre las solicitudes de los usuarios y el trabajo planificado para los equipos.

Administrador de proyectp:
- Gestionará los tiempos de las tareas con los equipos de desarrollo.
- Facilitará los espacios, recursos, tareas, y conversaciones necesarias para llevar a éxito los planes del proyecto.
- Revisará los indicadores en los equipos (se proponen métricas DORA).

Líder técnico:
- Facilitará y demostrará a los miembros del equipo de desarrollo del proyecto, las prácticas, guías de estilo definidas para la correcta ejecución del proyecto.
- Será responsable de la definición de los detalles técnicos que serán implementados para completar los requerimientos solicitados.
- Realizará actividades de desarrollo.

Desarrolladores de software:
- Desarrollará el producto de manera que sean identificables los cambios realizados para completar cada una de las tareas asignadas.
- Participará, opinará, y definirá, de manera activa los diseños técnicos necesarios para llevar los requerimientos de ideas a pasos concretos que las completen, así como las pruebas necesarias a realizar para demostrar que los criterios de aceptación de los requerimientos se cumplan.

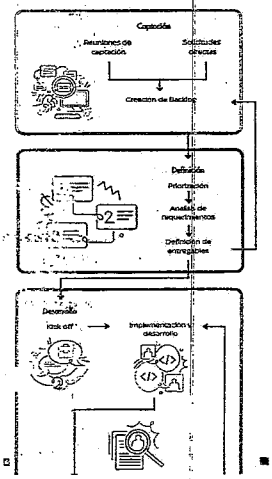
- Revisará que el código de sus compañeros complete los requerimientos en base a las guías de estilo y prácticas de codificación definidas para el proyecto.
- Reportará avances periódicos de sus avances en las tareas.

Aseguramiento de la calidad:

- Analizará los ambientes de desarrollo para demostrar y apoyar en la generación de evidencias de que los requerimientos han sido implementados y cumplidos bajo las expectativas de los criterios de aceptación definidos para cada una de ellas.
- Creará retroalimentación continua a los equipos de desarrollo en ciclos de mejora de calidad de producto.
- Apoyará en la revisión de manuales de usuario para demostrar que este manual cubre todo el conjunto de requerimientos solicitados.

Los roles que **BEEHIVE SYSTEMS S.A. DE C.V.** propone permiten llevar a cabo los flujos de trabajo con base en la estrategia de desarrollo trunk-based-development; sin embargo, en caso de que la convocante necesite roles adicionales e incluso algunos que no mencione en su Anexo Técnico, **BEEHIVE SYSTEMS S.A. DE C.V.** se compromete a entregar y poner a disposición dichos roles de tal manera que siempre se asegure la correcta ejecución y calidad de los servicios de desarrollo de software.

Diagrama de proceso del flujo de trabajo considerando las siguientes etapas:



Captación
Se propone como una etapa mediante la cual se identificarán y documentarán las necesidades de un proyecto para satisfacer a los usuarios y partes interesadas. Dependiendo la naturaleza del proyecto y la fase en la que se encuentra se podrá realizar la captación generalmente de dos maneras:

- A través de sesiones de captación
- A través de solicitudes generadas directamente por los usuarios

Como resultado de la etapa de captación, independientemente de la estrategia que se haya seguido para captar los requerimientos, todos estos deben estar documentados.

Definición
Se propone que tomando como entrada los requerimientos documentados en la etapa de captación, el equipo de desarrollo del proyecto junto con miembros del equipo interesado, ejecutarán una serie de reuniones para realizar la priorización y refinamiento de la definición de los requerimientos. Los objetivos de estas reuniones serán:

- Se propone determinar una lista ordenada de ejecución del desarrollo de los requerimientos para generar un producto gradual a lo largo del desarrollo del proyecto.
- Se propone identificar y documentar requerimientos faltantes al considerar aspectos técnicos más especializados.
- Se propone definirlar el "scope" de cada uno de los requerimientos, para que sea claro, conciso, y con un objetivo medible.
- Se propone describir cada uno de los criterios que se cumplirán para determinar que el producto satisface con lo solicitado una vez implementado.
- Se propone enumerar y describir cada uno de los entregables que se presentarán como evidencia de que las tareas satisfacen con el requisito solicitado y estas han sido finalizadas con éxito.

Como resultado de la etapa de definición, se tendrán tareas de alto nivel definidas para poder pasar al equipo de desarrollo.

Desarrollo
Se propone que en la etapa de desarrollo se tomen las tareas y elabore el código necesario para cumplir con los requisitos y criterios de aceptación, siguiendo el diseño y guías de estilo definidas para el proyecto y para cada una de sus tareas. Una vez finalizado el trabajo de codificación, el desarrollador creará una solicitud de revisión de su trabajo para que más miembros del equipo de desarrollo (incluyendo al Líder Técnico) la puedan revisar hasta que su trabajo sea aprobado

BEEHIVESYSTEMS
UNIFYING THE MANAGEMENT & SECURITY

Métricas de desempeño

- Tiempo de espera de cambio (Lead time): Medirá el tiempo que tarda el código comprometido en ejecutarse en producción, tiempo entre que llega a To Do al equipo de desarrollo y se completa la tarea.
- Ciclo de tiempo: Se propone como medición del tiempo que tarda la tarea en desarrollo (de "In progress" a "Done").
- Frecuencia de despliegue: Se medirá como el número de deploys / semana.
- Tasa de error de cambio: Se medirá como el número de deployments que se identifican como causa raíz de un error en el sistema.
- Tiempo medio de recuperación: Se implementará una medición que indique cuánto tiempo tarda en restablecerse un servicio después de un error.

Objetivos de implementar Trunk-Based-Development

- Se obtendrá retroalimentación más rápida de los cambios implementados a un sistema.
- Se reducirá la complejidad del código fuente que tiene que ser revisado, probado y aprobado.
- Se reducirá la complejidad de conflictos entre Merge Requests y la rama principal.
- Se implementarán mejores estrategias de testing. Los miembros del equipo podrán probar rápidamente las actualizaciones implementadas. Lo que permitirá identificar errores al momento de integrar con la rama principal.
- Se propone el control y mejoras en las estrategias de despliegue en ambientes de desarrollo/pruebas y producción.

Características del desarrollo basado en Trunk

- Desarrollar en iteraciones pequeñas: Se propone que un desarrollador realice por lo menos una o varias integraciones a la rama principal al día.

https://beehivesystems.mx contacto@beehivesystems.mx 33 2588 4412 / 33 8526 3103

BEEHIVESYSTEMS
UNIFYING THE MANAGEMENT & SECURITY

- Revisión de código síncrona: Se propone que los desarrolladores prioricen la revisión y aprobación de Merge Requests pendientes antes de seguir con su propio trabajo. Esto permitirá que sus compañeros no pasen a implementar otras funcionalidades con revisiones pendientes.
- Uso de feature flags: Se propone mantener el principio de trabajar con ramas de corta duración, esto permitirá que se realicen integraciones al código principal sobre funcionalidades que no se encuentran completas ni listas para ser utilizadas, o que provocarían errores en caso de estar activas. Para manejar esto, se propone el uso de condicionales que permitan habilitar o deshabilitar lógica de servicios o hacer que elementos de la interfaz de usuario sean visibles o no.
- Pruebas automatizadas: Se propone contar con pruebas automatizadas bien definidas, que permitirán validar la integridad del código fuente que se intenta integrar a la rama principal y permitirá obtener la velocidad del proceso de integración continua de cambios o actualizaciones que se espera al implementar el desarrollo basado en trunk.
- Pair programming: En ocasiones, dos programadores podrían trabajar en la misma tarea al mismo tiempo; en este escenario se propone que, tras analizar la problemática y llegar a una solución en conjunto, un desarrollador analice y revise la implementación que su compañero realiza, se entiende que el código ya ha sido revisado, lo que permitirá integrar directamente a la rama principal, o acelerará el proceso de revisión por otros compañeros y su integración.

Flujo de trabajo enfocado al desarrollo basado en Trunk

1. Se propone trabajar en una rama principal.
   - Todos los desarrolladores realizarán cambios o actualizaciones en ramas de corta duración a partir de una rama principal. Cómo mínimo se realizará una integración a la rama principal por día.
   - En cada actualización realizada al código fuente, los desarrolladores garantizarán que el o los sistemas afectados puedan ser desplegados y funcionarán correctamente en un ambiente de producción.
2. Se propone estrategia de branching.
   - Los desarrolladores trabajaran en actualizaciones o funcionalidades que puedan ser cargadas en la rama principal en un lapso no mayor a uno o dos días.
   - Funcionalidades más complejas o que requieren un esfuerzo mayor se separarán en tareas más pequeñas que permitirán cumplir con el punto anterior.
   - Comúnmente, se realizarán integraciones a la rama principal de tareas pequeñas que conforman una funcionalidad, sin embargo, mientras esto sucede la funcionalidad no estará completa y no estará lista para ser usada. Para estos escenarios, se utilizarán feature flags (o feature toggles).
   - Una vez una funcionalidad ha sido terminada, se eliminarán todas las feature flags usadas durante su implementación.
3. Se propone revisión de código fuente y Merge Requests (o Pull Requests).
   - El equipo de desarrollo se enfocará en contar con Merge Requests pequeños, que podrán ser revisados rápidamente y que incluiran pequeñas actualizaciones al código principal.
   - Todos los Merge Requests serán revisados en un lapso no mayor a 24 horas.

https://beehivesystems.mx contacto@beehivesystems.mx 33 2588 4412 / 33 8526 3103

BEEHIVESYSTEMS
UNIFYING THE MANAGEMENT & SECURITY

   - Los miembros del equipo darán prioridad a revisar los Merge Requests antes de comenzar a trabajar con nuevas tareas.
   - Todos los Merge Requests serán aprobados por al menos 2 miembros del equipo antes de integrarse a la rama principal.
4. Se propone integración continua.
   - Todos los Merge Requests pasarán por un proceso pipeline de CI.
   - Para cada Merge Request, se ejecutarán todas las pruebas automáticas existentes en el proyecto.
   - Si alguna prueba falla, el desarrollador que ha creado el Merge Request será responsable de corregir el origen del error de manera inmediata, deteniendo su trabajo actual de manera momentánea.
5. Se propone despliegue.
   - La rama principal estará siempre lista para su despliegue.
   - Se contará con un ambiente objetivo de despliegue continuo, donde se podrá revisar el estado del sistema tras cada integración de Merge Request creado por los desarrolladores.

https://beehivesystems.mx contacto@beehivesystems.mx 33 2588 4412 / 33 8526 3103

5.3.1. NUEVOS PROYECTOS

Como parte de los servicios para el desarrollo de nuevos proyectos, **BEEHIVE SYSTEMS S.A. DE C.V.** considera que se incluirán a modo enunciativo mas no limitativo, los siguientes tipos de proyectos, cuya necesidad podrá variar según el alcance de la solución o los requisitos específicos:

- Desarrollo de aplicaciones web.
- Desarrollo cliente-servidor.
- Desarrollo de aplicaciones móviles.
- Procesos background.
- Herramientas de intercambio de información (API's, Web Services y componentes de interconexión con otros servicios).

Los servicios solicitados serán desarrollados con los lenguajes, tecnologías, motores de bases de datos y modelos de inteligencia artificial que cumplan con lo establecido en la arquitectura base para desarrollo de sistemas y aplicaciones gubernamentales y serán avalados por la DIG de la DGITG.

5.3.2. MIGRACIÓN DE RECURSOS Y APLICACIONES EXISTENTES

Con respecto a los recursos o aplicaciones que se encuentran fuera de la nueva arquitectura base para desarrollo de sistemas y aplicaciones gubernamentales, **BEEHIVE SYSTEMS S.A. DE C.V.** realizara los trabajos de adecuación que permitan integrar y migrar a estos recursos o aplicaciones a la nueva arquitectura. Para estimar el costo en horas de los trabajos de migración de recursos o aplicaciones existentes se utilizará el mecanismo establecido en el punto de 5.1.5. ESTIMACIÓN DE HORAS. En cualquiera de los casos de migración de recursos o aplicaciones, se incluirá las garantías para cubrir posibles errores o vicios ocultos que pudieran presentarse posterior a la liberación del producto.

5.3.3. OTROS SERVICIOS

Para aquellos casos en que la DIG de la DGITG necesite alguna solución o servicio que no esté descrito en el presente Anexo Técnico, podrá realizar la solicitud a través de una sesión presencial o virtual con **BEEHIVE SYSTEMS S.A. DE C.V.** Para estimar el costo en horas de los trabajos de otros servicios, se utilizará el mecanismo establecido en el punto de 5.1.5. ESTIMACIÓN DE HORAS.

5.4. SEGURIDAD DEL CÓDIGO

BEEHIVE SYSTEMS S.A. DE C.V. considera una base de conocimientos sobre seguridad del código relacionada con procesos, métricas y herramientas aplicadas durante el Ciclo de Vida de Desarrollo de

Software (SDLC) para identificar, mitigar y prevenir vulnerabilidades desde la concepción del código fuente y durante la duración de su ciclo de vida. El objetivo de contar con esta base de conocimientos es mejorar el porcentaje de operación de las aplicaciones, incrementando la resiliencia ante ataques intencionados o errores accidentales, aumentando la seguridad de la información en aspectos como la confidencialidad, integridad y disponibilidad.

A continuación, se presentan los servicios técnicos particulares que son considerados por BEEHIVE **SYSTEMS S.A. DE C.V.** en esta propuesta.

5.4.1. ANÁLISIS ESTÁTICO DE SEGURIDAD DE APLICACIONES (SAST)

BEEHIVE SYSTEMS S.A. DE C.V. realizara revisiones automatizadas de código fuente; el objetivo es identificar vulnerabilidades de seguridad de forma temprana en el ciclo de vida de desarrollo (Shift Left Security), de esta manera se identificarán fallos críticos como inyección SQL, Cross-Site Scripting (XSS), gestión insegura de secretos (passwords en código) y uso de criptografía débil. **BEEHIVE SYSTEMS S.A. DE C.V.** recomienda estándares como OWASP Top 10 o SANS CWE Top 25.

5.4.2. MEDICIÓN DE LA CALIDAD DEL CÓDIGO

BEEHIVE SYSTEMS S.A. DE C.V. realizará revisiones de los componentes del software para asegurar que estos cumplen con estándares de codificación; dicho código contará con una estructura que permita a la DIG de la DGITG medir y avalar aspectos de legibilidad, mantenibilidad y eficiencia del código, garantizando que la DIG de la DGITG pueda leer, entender y mantener el código sin depender de **BEEHIVE SYSTEMS S.A. DE C.V.**, lo que brindará gobernanza sobre los proyectos y soluciones de la Póliza de Desarrollo, Mantenimiento y Soporte a los Sistemas y Procesos Informáticos con Fábrica de Software.

5.4.3. GESTIÓN TÉCNICA Y MÉTRICAS DE REFACTORIZACIÓN

BEEHIVE SYSTEMS S.A. DE C.V. realizará revisiones sobre el tiempo y recursos que pudieran ser necesarios para corregir las funcionalidades implementadas en el proyecto de tal manera que la DIG de la DGITG pueda determinar un tiempo activo de vida del proyecto antes de requerir trabajos de mantenimiento o refactorización, evitando que este se convierta en un lastre costoso. **BEEHIVE SYSTEMS S.A. DE C.V.** recomienda y propone la revisión de indicadores como clases o métodos gigantes en el código, código muerto, obsolescencia y comentarios/descripciones del código con el objetivo de que la DIG de la DGITG pueda avalar (en caso de ser necesario) que el proyecto cumple con los parámetros de tiempo y costo que esta podría invertir para refactorizar el proyecto o mantener activo el proyecto.

Con el objetivo de avalar que **BEEHIVE SYSTEMS S.A. DE C.V.** cuenta con experiencia en la implementación de mecanismos de SEGURIDAD DEL CÓDIGO, presentamos como parte de nuestra propuesta un documento en el que describimos cómo implementaremos prácticas de desarrollo seguro y pruebas de software. El documento incluye los puntos o elementos siguientes:

- Qué son las prácticas generales para el desarrollo seguro
- Beneficios de implementación de buenas prácticas de desarrollo seguro

- Lista de verificación de prácticas de codificación segura:
  - Validación de entradas (Input validation)
  - Codificación de salidas (Output encoding)
  - Administración de autenticación y contraseñas
  - Administración de sesiones
  - Control de acceso
  - Manejo de errores y logs
  - Protección de datos
  - Seguridad de las comunicaciones
  - Configuración de los sistemas
  - Seguridad de base de datos
  - Manejo de archivos
- Pruebas de software
  - Principios básicos
  - Tipos de pruebas
  - Buenas prácticas
  - Ubicación de las pruebas
  - Que probar y que no
  - Ejemplo

DESCRIPCIÓN DE IMPLEMENTACIÓN DE PRÁCTICAS DE DESARROLLO SEGURO Y PRUEBAS DE SOFTWARE

Qué son las prácticas generales para el desarrollo seguro

Para definir correctamente que son las practicas generales para el desarrollo seguro, se requiere responder a las siguientes preguntas: ¿Qué es? ¿Para qué? Y ¿Cómo?
Qué es: Son metodologías en las cuales se considera la seguridad de la aplicación durante todo su ciclo de vida.
Para qué: Se busca minimizar los riesgos de la exposición de vulnerabilidades o amenazas mientras se desarrolla una aplicación
Cómo: Implementando prácticas de desarrollo seguro y mejora continua de los procesos de desarrollo.

Estas prácticas ayudan a mitigar riesgos y vulnerabilidades comunes que podrían ser explotadas por atacantes en etapas tempranas de la programación de una aplicación.
El desarrollo de software se centra principalmente en el funcionamiento de algoritmos para tareas específicas; sin embargo, hoy en día es bien sabido que una mala redacción del código de los programas a menudo también da lugar a problemas de seguridad. Durante el proceso de programación, las prácticas de codificación y las técnicas de programación estructurada desempeñan un papel primordial, teniendo en cuenta el caso de uso específico y sus necesidades de seguridad, las técnicas de diseño inseguras deben prohibirse sistemáticamente y el código debe documentarse y revisarse adecuadamente para eliminar los fallos relacionados con la seguridad, de tal manera que debe evaluarse el análisis realizado a los errores de programación más comunes y la documentación de su corrección.

Beneficios de implementación de buenas prácticas de desarrollo seguro

La implementación de buenas prácticas de desarrollo seguro traerá como beneficio:

- Software más seguro.
  Al considerar la seguridad desde el inicio del ciclo de vida del software, se reducirá el número de vulnerabilidades y su criticidad.
- Detección temprana de fallos.
  Permitirá identificar y corregir vulnerabilidades en etapas tempranas del desarrollo y disminuirá el riesgo en los ambientes de pruebas y producción
- Reducción de costos.
  La detección temprana y resolución de problemas de seguridad son menos costosos en las etapas tempranas del desarrollo. Por ejemplo, corregir una vulnerabilidad de inyección de código, o inyección sql al momento de estar desarrollando es menos costoso que corregirlo después de detectarlo por una exposición de datos personales no autorizada.
- Reducción de riesgos para la convocante.
  Al reducir la posibilidad de recibir ataques por la aplicación, se disminuirá también la posibilidad de que la convocante se vea afectada.
- Aumento de satisfacción de la convocante.
  Al realizar entregas con menos fallos y menos vulnerabilidades, es muy probable el aumento de satisfacción de la convocante.

Lista de verificación de prácticas de codificación segura:

BEEHIVE SYSTEMS S.A. DE C.V. propone las siguientes verificaciones como prácticas de codificación segura:

- Validación de entradas (Input validation):
  La validación de entradas es una defensa básica pero esencial contra muchos tipos de ataques y errores en las aplicaciones, protegerán tanto a los usuarios como a la aplicación y sistemas. Se refiere al proceso de asegurarse de que los datos proporcionados por un usuario o un sistema externo sean correctos, esperados y seguros antes de ser procesados o utilizados por la aplicación.
  Se propone la implementación y ejecución de las siguientes validaciones:
  - Existirá una rutina de validación de datos de entrada centralizada para la aplicación.
  - Se especificarán sets de caracteres apropiados, tales como UTF-8, para todas las fuentes de entrada.
  - Todas las fallas en la validación terminarán en el rechazo del dato de entrada.
  - Se codificarán los datos a un set de caracteres común antes de validar (Canonicalización).

- Se validarán tipos de datos no esperados.
- Se validarán rangos de datos.
- Se validarán largos de datos.
- Si es necesario, se permitirá el ingreso de algún carácter considerado peligroso, asegurando la implementación de controles adicionales tales como la codificación de la salida, API de seguridad y el registro del uso de tales datos a lo largo de la aplicación. Entre los ejemplos de caracteres peligrosos podemos encontrar:< > " ' % ( ) & + \ /\'\"

- Codificación de salidas (Output encoding):

  Implicará el transformar o "codificar" los datos que una aplicación genera y envía de vuelta al usuario o un sistema externo, para que no se interpreten como código ejecutable en el navegador u otro contexto. La codificación convertirá los caracteres especiales en representaciones seguras que no se procesan como código.

  Se propone la implementación y ejecución de las siguientes validaciones:
  - Se utilizará una rutina probada y estándar para cada tipo de codificación de salida.
  - Se codificarán todos los caracteres salvo que sean reconocidos como seguros por el interpretador al que están destinados.
  - Se propone sanitizar contextualmente todas las salidas de datos no confiables hacia consultas SQL.
  - Se propone sanitizar todas las salidas de datos no confiables hacia un comando del sistema operativo.

- Administración de autenticación y contraseñas:

  La autenticación se refiere al proceso mediante el cual un sistema verifica la identidad de un usuario, y las contraseñas son uno de los métodos más comunes para este propósito. Gestionar contraseñas de forma segura es un desafío constante, ya que las contraseñas suelen ser un punto crítico de vulnerabilidad si no son manejadas y almacenadas de manera adecuada.

  Se propone la implementación y ejecución de las siguientes validaciones:
  - Se solicitará la autenticación para todos los recursos y páginas excepto aquellas específicamente clasificadas como públicas.
  - Se establecerán y utilizarán servicios de autenticación estándares y probados cuando sea posible.
  - Se propone utilizar una implementación centralizada para todos los controles de autenticación.
  - Todos los controles de autenticación fallarán de una forma segura (para las ocasiones en que se presenten fallas).
  - Si la aplicación administra un almacenamiento de credenciales, se asegurará que únicamente se almacene el hash con sal (salty hash) de las contraseñas y que el

archivo/tabla que guarda las contraseñas y claves solo puede ser escrito por la aplicación.
- El hash de las contraseñas será implementado en un sistema en el cual se confíe.
- Se validarán los datos de autenticación únicamente luego de haber completado todos los datos de entrada, especialmente en implementaciones de autenticación secuencial.
- Se utilizará autenticación para conexiones a sistemas externos que involucren información o funciones sensibles.
- Se utilizarán únicamente solicitudes del tipo HTTP POST para la transmisión de credenciales de autenticación.
- Se propone que se considere que el código fuente no es una ubicación segura para almacenar credenciales.
- Se utilizarán únicamente conexiones encriptadas o datos encriptados para el envío de contraseñas, contraseñas temporales como aquellas asociadas con reseteos por correo electrónico, pueden ser una excepción.
- Se propone contar con políticas o regulación de complejidad de la contraseña.
- Las contraseñas serán suficientes para resistir ataques típicos de las amenazas al sistema. Ejemplo: longitud mínima de 12 caracteres, combinación de caracteres numéricos / alfanuméricos / caracteres especiales.
- Se considerará en medida de lo posible utilizar frases de varias palabras para la contraseña y superar longitudes de 16 caracteres.
- No se desplegará en la pantalla la contraseña ingresada.
- Las contraseñas y links temporales tendrán un corto periodo de validez.
- Se propone prevenir la reutilización de contraseñas.
- Se hará cumplir por medio de una política o regulación los requerimientos de cambio de contraseña.
- Se propone re-autenticar usuarios antes de la realización de operaciones críticas.
- Se utilizará autenticación multi-factor por lo menos para las cuentas más sensibles o de mayor valor.
- Si se utiliza una librería de terceros para la autenticación, se realizará una inspección minuciosa para asegurar que no se encuentra afectado por cualquier código malicioso.

- Administración de sesiones

  Este es un componente crítico de la seguridad en las aplicaciones web, ya que las sesiones permiten mantener el estado de autenticación de un usuario a lo largo de múltiples solicitudes sin requerir que el usuario se autentique en cada una de ellas; sin embargo, las sesiones mal administradas pueden ser una puerta de entrada para varios tipos de ataques. Entre ellos session hijacking y CSRF (Cross-site request forgery).

Se propone la implementación y ejecución de las siguientes validaciones:
- Se usarán identificadores de sesión aleatorios y seguros, se recomienda el uso de algoritmos suficientemente aleatorios.
- Se propone que la creación de los identificadores de sesión sea realizada en un sistema en el cual se confíe.
- Se usarán cookies seguras para almacenar los IDs de sesión.
- Se propone el uso de tiempos de expiración de sesiones adecuado al negocio; es decir, que sea lo más corto posible, balanceando los riesgos con los requerimientos del negocio.
- Si el sistema utiliza algún mecanismo de re-autenticación, se generará un nuevo identificador de sesión y garantizará que el identificador anterior sea eliminado.
- En medida de lo posible, no se permitirán inicios de sesión concurrentes con el mismo usuario, en caso de manejarlos, se validará que cada inicio de sesión utiliza un identificador diferente y estos serán auditados.
- Se validará el origen de las solicitudes.
- El cierre e inicio de sesión será mediante protocolos seguros (para aplicaciones web garantizar se utiliza HTTPS).
- Se propone implementar protección contra ataques de session hijacking como ejemplo utilizar tokens anti-CSRF, uso de HTTPS y prevenir el acceso de sesiones desde diferentes direcciones IP (por ejemplo, una dirección IP por sesión)
- Se realizará monitoreo y auditoría de uso de sesiones.
- En el caso de operaciones sensibles (cambios de contraseña, configuraciones de seguridad de la aplicación), se solicitará la re-autenticación del usuario antes de que el usuario realice la acción.

- Control de acceso

  Se encargará de asegurar que solo los usuarios autorizados puedan acceder a recursos específicos, funcionalidades o datos dentro de la aplicación. Implementar un control de acceso adecuado es crucial para evitar vulnerabilidades como la exposición de información sensible, elevación de privilegios y accesos no autorizados. Un control de acceso implementado tomando en cuenta buenas prácticas de seguridad, asegurará que los usuarios solo puedan realizar las acciones para las que están autorizados, basándose en su identidad, rol y permisos.

  Se propone la implementación y ejecución de las siguientes validaciones:
  - Se utilizará un único componente para el chequeo de autorizaciones para todo el sitio.
  - Se propone establecer controles basados en roles (RBAC), basado en atributos (ABAC) o basado en políticas (PBAC) y persistirlo en toda la aplicación, la elección de estos controles dependerá de la definición técnica y reglas de negocio de la aplicación.
  - Los controles de acceso en caso de falla actuarán en forma segura.
  - Se propone denegar todos los accesos en caso de que la aplicación no pueda acceder a la información de configuración de seguridad.
  - Se restringirá el acceso a URLs protegidas, solo a usuarios autorizados.

- Se restringirá el acceso a funciones protegidas, solo a usuarios autorizados.
- Se restringirá las referencias directas a objetos, solo a usuarios autorizados.
- Se restringirá el acceso a servicios, solo a usuarios autorizados.
- Se restringirá el acceso a información de la aplicación, solo a usuarios autorizados.
- Se restringirá el acceso a usuario, atributos y política de información utilizada por los controles de acceso.
- Las reglas de control de acceso implementadas del lado del servidor (backend) y en la capa de presentación (frontend), coincidirán.
- Si sesiones de autenticación extensas son permitidas, periódicamente se re-validará la autorización de los usuarios y asegurará que sus privilegios no han sido modificados.
- Se propone crear una política de control de acceso para documentar las reglas del negocio de la aplicación.

- Manejo de errores y logs

  Esta medida es esencial para proteger la aplicación de posibles riesgos de seguridad. Cuando una aplicación no maneja correctamente los errores, se pueden exponer detalles internos del sistema que faciliten un ataque, o abuso del sistema, a su vez el manejo de logs de manera correcta ayudará en la fase de detección de vulnerabilidades y / o riesgos y por este medio podrán ser corregidos.

  Se propone la implementación y ejecución de las siguientes validaciones:

  Para errores:
  - No se revelarán detalles sensibles en los mensajes de error (Contraseñas, cadenas de conexión, variables de entorno).
  - No se mostrará información técnica al usuario en los mensajes de error (error de base de datos, error de consulta a un API).
  - Se propone centralizar el manejo de errores en el código fuente, de preferencia que los errores se validen en el retorno a los usuarios y manejarlos mediante códigos o etiquetas para su identificación sin revelar información sensible.
  - Para errores no esperados de la aplicación, se implementarán mensajes de error genéricos.
  - Se utilizarán códigos de respuesta HTTP adecuados para el tipo de error.
  - Se propone que la gestión de errores este asociada a los controles de seguridad (errores de autenticación y control de accesos).

  Para logs:
  - Se restringirá el acceso a los logs, solo a personal autorizado.
  - Los logs de control de acceso incluirán casos de éxito y fallas.
  - Se propone centralizar el manejo de logs en el código fuente, existirá una rutina para generar los logs.
  - No se guardará información sensible en logs (esto incluye información de usuario y especificaciones del sistema).
  - Se propone mantener niveles de log según la severidad del evento.

- Se propone evitar que los logs sean información repetitiva.
- Se propone mantener políticas de rotación, retención y eliminación de logs.
- Se registrarán en un log todas las fallas de validación.
- Se registrará en un log todos los intentos de autenticación.
- Se registrarán en un log todas las fallas en los controles de acceso.
- Se registrarán en un log todas las excepciones del sistema.
- Se registrará en un log los intentos de evasión de controles.
- Se registrarán en un log todas las funciones administrativas, incluyendo cambios en la configuración de seguridad.
- Se utilizarán funciones hash para validar la integridad de los logs.

- Protección de datos

  Este punto se refiere a la protección de los datos mediante mecanismos utilizados para garantizar la confidencialidad, integridad y disponibilidad de la información dentro de la aplicación. Las aplicaciones modernas procesan y almacenan grandes volúmenes de información sensible, dependiendo del fin que tenga la aplicación y las necesidades del negocio, esta información sensible puede contener datos personales, financieros e incluso de salud de sus usuarios, proteger estos datos es crucial para evitar violaciones de privacidad, perdida de datos y exposición no autorizada.

  Se propone la implementación y ejecución de las siguientes validaciones:
  - Se implementará el mínimo privilegio, restringir el acceso de los usuarios solamente a la funcionalidad, datos y sistemas de información que son necesarios para realizar sus tareas.
  - Se propone encriptar toda la información altamente sensible almacenada en reposo.
  - Se propone encriptar toda la información en tránsito entre el cliente y servidor, así como la comunicación de esta información entre sistemas que deban utilizarla.
  - Toda encriptación utilizará algoritmos de encriptación que hayan sido validados y con buenos antecedentes.
  - No se almacenarán contraseñas, cadenas de conexión u otra información sensible en texto claro o de forma que sean visibles del lado del cliente.
  - Se deshabilitarán las funcionalidades de completar automáticamente en aquellos formularios que contienen información sensible.
  - La aplicación soportará la eliminación de datos sensibles cuando los datos ya no son requeridos.
  - Se implementarán controles de accesos apropiados para los datos sensibles almacenados en el servidor.
  - Se cumplirá con normativas de privacidad para garantizar que los datos sean procesados de forma ética y legal.

- Seguridad de las comunicaciones

BEEHIVESYSTEMS
UNIFYING THE MANAGEMENT & SECURITY

Con este punto se garantizará que los datos intercambiados entre los clientes y servidores, así como entre componentes de la infraestructura, se mantengan confidenciales. Si las comunicaciones no están adecuadamente protegidas, pueden ser interceptadas, manipuladas o utilizadas para llevar a cabo ataques como el man-in-the-middle, spooing e inyección de datos.

Para las aplicaciones web es de especial importancia el uso del Protocolo de Transferencia del Hipertexto Seguro (HTTPS) esto para garantizar que los datos no puedan ser leídos o modificados durante su transmisión.

Se propone la implementación y ejecución de las siguientes validaciones:
- Los certificados TLS serán válidos y contendrán el nombre de dominio correcto.
- No se utilizarán certificados expirados y serán instalados con los certificados intermedios si son requeridos.
- Las conexiones TLS que fallen no se transformaran en una conexión insegura.
- Se utilizarán conexiones TLS para todo el contenido que requiera acceso autenticado y para todo otro tipo de información sensible.
- Se utilizará una única implementación estándar de TLS que se encontrará configurada correctamente.
- Se especificarán los caracteres de codificación para todas las conexiones.
- Se implementará encriptación para todas las transmisiones de información sensible.

- Configuración de los sistemas

  Abarcará una serie de prácticas y principios que ayudarán a asegurar que tanto el software como su entorno de ejecución sean lo más seguros posibles, minimizando las vulnerabilidades y riesgos de seguridad. Este punto es un proceso multidisciplinario que abarca desde la infraestructura hasta el código fuente, implica no solo proteger las aplicaciones y los datos; sino también, configurar adecuadamente los servidores, redes y componentes del sistema para reducir la posibilidad de un ataque.

  Se propone la implementación y ejecución de las siguientes validaciones:
  - Se garantiza que los servidores, los frameworks y los componentes del sistema estarán corriendo la última versión aprobada.
  - Se garantiza que los servidores, los frameworks y los componentes del sistema estarán actualizados con todos los parches emitidos para las versiones en uso.
  - Se removerán todas las funcionalidades y archivos que no sean necesarios.
  - Se propone restringir el servidor web, los procesos y las cuentas de servicios con el mínimo privilegio posible.
  - Se removerá el código de pruebas o cualquier funcionalidad que no sea tenida en cuenta en producción, previo a realizar la puesta en producción.
  - Se definirá cuáles de los métodos HTTP, GET o POST, soportará la aplicación y si serán manejados de forma diferente en las distintas páginas de la aplicación.
  - Se removerá información innecesaria en los cabezales de HTTP de respuesta referidas al SO, versión del servidor web y frameworks de aplicación.

https://beehivesystems.mx contacto@beehivesystems.mx 33 1588 4412 / 33 8526 3103

BEEHIVESYSTEMS
UNIFYING THE MANAGEMENT & SECURITY

- Se propone aislar los ambientes de desarrollo de los ambientes de producción, permitiendo el acceso solamente a los grupos de desarrollo y pruebas a específicamente autorizados.
- Se implementará un Sistema de Control de Cambios del Software para manejar y registrar los cambios al código tanto para los ambientes de desarrollo como para los de producción.
- No se utilizará configuración por defecto a servicios que sean utilizados por la aplicación.
- A los ambientes de pruebas y producción públicos; es decir, que tengan acceso a internet, se les realizará un endurecimiento del sistema.

- Seguridad de base de datos

  Las bases de datos contienen a menudo la información más sensible de una aplicación, si un atacante logra acceder a la base de datos, puede comprometer toda la aplicación y exponer información confidencial.

  Se propone la implementación y ejecución de las siguientes validaciones:
  - Se utilizarán consultas parametrizadas con tipos de datos fuertemente tipados.
  - Se garantiza que todas las variables tendrán tipos de datos asociados.
  - Las cadenas de conexión a la base de datos no estarán incluidas en el código de la aplicación.
  - Se utilizarán procedimientos almacenados para abstraer el acceso a los datos y eliminarán los permisos de las tablas en la base de datos.
  - Se deshabilitarán las cuentas por default / adicionales que no son necesarias para la operativa del negocio.
  - Se deshabilitarán todas las funcionalidades innecesarias de la base de datos.
  - La aplicación se conectará a la base de datos con credenciales diferentes para cada nivel de confianza.
  - Se utilizarán credenciales seguras para acceder a la base de datos.
  - Se limitará la conexión a la base de datos mediante listas de control de acceso, para que solo sea accesible por los componentes o sistemas que deben poder conectarse.

- Manejo de archivos

  Los archivos que se encuentran dentro del servidor o la aplicación pueden contener información sensible o ser un vector de ataque si no se gestionan adecuadamente. Un manejo inapropiado de archivos puede permitir a los atacantes realizar ejecuciones remotas de código, exposición de datos sensibles o incluso acceso no autorizado a los recursos del sistema.

  Se propone la implementación y ejecución de las siguientes validaciones:
  - No se utilizará directamente información provista por el usuario en ninguna operación dinámica.
  - Se exigirá autenticación antes de permitir la transferencia de un archivo al servidor.

https://beehivesystems.mx contacto@beehivesystems.mx 33 1588 4412 / 33 8526 3103

BEEHIVESYSTEMS
UNIFYING THE MANAGEMENT & SECURITY

- Se permitirá transferir al servidor únicamente los tipos de archivo (por ejemplo: pdf, doc, etc) requeridos por la operativa del negocio.
- Se validarán los tipos de archivo transferidos verificando la estructura de los encabezados.
- No se guardarán los archivos transferidos en el mismo contexto que la aplicación web.
- Se eliminarán los permisos de ejecución a los archivos transferidos.
- No se utilizará información provista por el usuario para la generación de redirecciones dinámicas. Si se debe proveer esta funcionalidad, la redirección aceptará únicamente caminos relativos dentro de la URL previamente establecidos.
- No se incluirá en parámetros nombres de directorios o rutas de archivos
- Nunca se enviará la ruta absoluta de un archivo al cliente.
- Se garantiza que los archivos y recursos de la aplicación sean de solo lectura.
- Se revisarán los archivos transferidos por los clientes en busca de virus y malware.

Pruebas de software

BEEHIVE SYSTEMS S.A. DE C.V. propone considerar los siguientes aspectos relacionados con pruebas de software:

Principios básicos
- Confiabilidad: Las pruebas serán repetibles y consistentes.
- Aislamiento: Cada prueba podrá ejecutarse independientemente, es decir, el resultado de cualquier par de pruebas A y B, debe ser el mismo si se ejecuta A antes que B y si se ejecuta B antes que A.
- Automatización: De preferencia, se integrará la ejecución de las suites de pruebas en los pipelines de CI/CD.
- Cobertura: Tener 100% de cobertura es difícil y laborioso, se priorizarán pruebas en funciones críticas que den más confianza de que el código hace lo que se espera, por ejemplo, en procesos de ejecución que pueden ser tardados, y en aquellos que la implementación del código no es trivial.

Tipos de pruebas
- Unitarias: Probarán unidades de código. Si bien la definición de unidad siempre ha sido debatible, se propone no definir una unidad como una función o un módulo, esto permitirá afirmar que no es necesario probar funciones privadas si se cubren indirectamente por una prueba de otra función que no es privada. En general, nuestras unidades como nuestro código se basarán más en la funcionalidad, más adelante se ve un ejemplo de prueba unitaria para un módulo de autenticación usando JWT, si bien las pruebas no cubren todos los escenarios, esta prueba se realizó para mostrar la idea de unidad como funcionalidad. De nada sirve probar que la librería de JWT entrega un token JWT eso lo debe cubrir la librería), así como no abona mucho demostrar que la librería puede validar un JWT. Lo que nos interesa es poder demostrar que un token JWT generado y

https://beehivesystems.mx contacto@beehivesystems.mx 33 1588 4412 / 33 8526 3103

validado con el mismo secreto es válido, y que con un secreto diferente no lo es, aquí probaremos la funcionalidad de validación utilizando las funciones de generación de Token y verificación de Token, no las funciones como tal.

- Integración: Verificarán la comunicación entre módulos y servicios. Estas demostrarán que el sistema se conecta a la base de datos que espera, que puede ejecutar consultas sobre esta, y que si hace peticiones a otro sistema estos también regresarán y recibirán los datos que enviamos sin generar problemas. Si bien estos pueden generar dependencia de infraestructura para ser probado, hay mecanismos de despliegue que lo pueden facilitar. En general, además de probar conexiones, buscamos probar que los contratos con estos sistemas no se han roto (permitiéndonos utilizar este conjunto de pruebas como una especie de capa "anticorrupción"). En estas pruebas podemos por ejemplo inspeccionar que las respuestas que nos entregan los servicios funcionan.
- End-to-End: Simularán flujos completos desde la perspectiva del usuario. Estas pruebas, idealmente ayudarán a automatizar el trabajo de validación del sistema. Ejecutando cada uno de los pasos que el usuario debe realizar en el sistema para probar que cumple con las características que se esperan.

Buenas prácticas

- Se propone usar herramientas recomendadas para cada stack.
- Se propone el uso de nombres descriptivos y pruebas simples.
- Se propone limpiar datos después de cada prueba.

Ubicación de las pruebas

- Unitarias: Se propone que se ubiquen cerca del archivo de código correspondiente.
- Integración/E2E: Se propone que se ubiquen en una estructura orientada a funciones o servicios.

Que probar y que no

- Probar: Se proponen las pruebas de lógica de negocio, validaciones, interacciones.
- No probar: Se propone no asumir la responsabilidad por las pruebas y el resultado de las pruebas de implementaciones de terceros o código temporal.

Ejemplo

- El siguiente ejemplo es una prueba unitaria (TypeScript + Jest)

```
import jwt from 'jsonwebtoken';
export const generateToken = (payload: object, secret: string): string => jwt.sign(paylo
ad, secret);
const verifyToken = (token: string, secret: string): boolean => { try { jwt.verify(toke
n, secret); return true; } catch { return false; } };
export const validateUserToken = (token: string, secret: string): boolean => verifyToken
(token, secret);


import { validateUserToken, generateToken } from './jwtService';
const SECRET = 'mi_secreto_aes';
describe('validateUserToken', () => {
  it('valida token con secreto correcto', () => {
    const token = generateToken({ userId: 1 }, SECRET);
    expect(validateUserToken(token, SECRET)).toBe(true);
```


BEEHIVESYSTEMS
UNIFYING THE MANAGEMENT & SECURITY

```
import jwt from 'jsonwebtoken';
export const generateToken = (payload: object, secret: string): string => jwt.sign(payload, secret);
const verifyToken = (token: string, secret: string): boolean => { try { jwt.verify(token, secret); return true; } catch { return false; } };
export const validateUserToken = (token: string, secret: string): boolean => verifyToken(token, secret);

import { validateUserToken, generateToken } from './jwtService';
const SECRET = 'mi_secreto_aes';
describe('validateUserToken', () => {
  it('valida token con secreto correcto', () => {
    const token = generateToken({ userId: 1 }, SECRET);
    expect(validateUserToken(token, SECRET)).toBe(true);
  });
  it('rechaza token con secreto incorrecto', () => {
    const token = generateToken({ userId: 1 }, 'otro_secreto');
    expect(validateUserToken(token, SECRET)).toBe(false);
  });
});
```

https://beehivesystems.mx contacto@beehivesystems.mx 33 1588 4412 / 33 8526 3103

BEEHIVESYSTEMS
UNIFYING THE MANAGEMENT & SECURITY

5.5. NIVELES DE SERVICIO

BEEHIVE SYSTEMS S.A. DE C.V. se compromete a establecer un nivel de servicio (SLA) con los siguientes niveles de prioridades para incidentes y servicios:

Prioridades para incidentes:

Prioridad	Descripción	Tiempo de Respuesta	Tiempo de Solución
0 - Crítica	El problema ha causado la imposibilidad de continuar trabajando completa e inmediatamente, afectando procesos de negocio críticos o a un grupo completo de usuarios tales como: una administración completa, servicio de negocio o procedimiento crítico.	Inmediato	Inmediato
1 - Alta	Un proceso de negocio es afectado de tal forma que exista una severa degradación de sus funciones, un grupo de usuarios está afectado o un usuario crítico	2 horas	4 horas

https://beehivesystems.mx contacto@beehivesystems.mx 33 1588 4412 / 33 8526 3103

BEEHIVESYSTEMS
UNIFYING THE MANAGEMENT & SECURITY

	está afectado. Pueden existir alternativas de trabajo; sin embargo, no son sostenibles de manera fácil.		
2 - Media	Un proceso de negocio es afectado de tal forma que exista falta de disponibilidad de funciones para los usuarios finales o la calidad del servicio en un sistema se vea degradado. Pueden existir alternativas de trabajo.	4 horas	8 horas
3 - Baja	El proceso tiene un bajo impacto en la operación del negocio y su atención y solución puede ser calendarizada; existen alternativas de trabajo.	8 horas	16 horas

Prioridades para servicios:

Prioridad	Descripción	Tiempo de Respuesta	Tiempo de Solución
0 - Crítica	En caso de que el servicio haya sido solicitado por algún usuario crítico de la convocante, o servicio crítico, la solicitud será considerada de prioridad crítica.	Inmediato	Inmediato
1 - Alta	De no ser atendido, el servicio podrá bloquear la operación, afectar algún proceso de negocio o algún desarrollo en curso.	2 horas	4 horas
2 - Media	Un proceso de negocio es afectado de tal forma que exista falta de disponibilidad de funciones para los usuarios finales o la calidad del servicio en un sistema se vea degradado. Pueden existir alternativas de trabajo.	4 horas	8 horas

https://beehivesystems.mx contacto@beehivesystems.mx 33 1588 4412 / 33 8526 3103

3 - Baja	El Servicio debe ser atendido lo antes posible para evitar posibles afectaciones en algún proceso de negocio o afectar la dependencia con algún otro desarrollo.	8 horas	16 horas

5.6. CONSIDERACIONES GENERALES

- Confidencialidad
  - **BEEHIVE SYSTEMS S.A. DE C.V.** se compromete y acepta la obligación a guardar estricta confidencialidad respecto de toda la información, datos, documentos, sistemas, procesos, infraestructura y cualquier otro elemento al que tenga acceso con motivo de la presente licitación, independientemente de su naturaleza o medio de almacenamiento. Dicha obligación es indefinida, manteniéndose vigente aun después de la terminación del contrato, por cualquier causa.
  - **BEEHIVE SYSTEMS S.A. DE C.V.** implementará, mantendrá y demostrará la existencia de medidas de seguridad administrativas, técnicas y físicas suficientes para garantizar la protección de la información, conforme a mejores prácticas y normativa aplicable en materia de protección de datos.
  - **BEEHIVE SYSTEMS S.A. DE C.V.** acepta y confirma que queda estrictamente prohibida la reproducción, divulgación, transferencia, comercialización o uso indebido de la información sin autorización previa y por escrito de la convocante.
  - **BEEHIVE SYSTEMS S.A. DE C.V.** se compromete a ser responsable directo por cualquier vulneración, fuga de información, acceso no autorizado o incumplimiento en materia de confidencialidad, incluyendo los actos de su personal, subcontratistas o terceros relacionados.
  - En caso de incidente de seguridad, **BEEHIVE SYSTEMS S.A. DE C.V.** notificará de manera inmediata a la convocante y ejecutará acciones correctivas y de mitigación sin perjuicio de las sanciones correspondientes.

- Autonomía operativa de la DIG de la DGITG:
  - **BEEHIVE SYSTEMS S.A. DE C.V.** se compromete a no establecer restricciones técnicas, legales y/o comerciales que obliguen a la convocante a mantener una relación más allá de la vigencia del contrato con **BEEHIVE SYSTEMS S.A. DE C.V.**
  - Bajo ninguna circunstancia podrá generarse dependencia tecnológica o contractual hacia **BEEHIVE SYSTEMS S.A. DE C.V.** , por lo que **BEEHIVE SYSTEMS S.A. DE C.V.** no condicionará la operación o desarrollo del software a su participación exclusiva.
  - **BEEHIVE SYSTEMS S.A. DE C.V.** se compromete a no retener ninguna información recolectada en la captación, definición, desarrollo y cierre de cualquiera de los sistemas desarrollados en esta licitación; toda la información generada, procesada o utilizada durante el ciclo de vida del proyecto será entregada de forma íntegra, estructurada y accesible a la DIG de la DGITG, sin reservas ni limitaciones.

- Derechos de la DIG de la DGITG sobre el software:

BEEHIVESYSTEMS
UNIFYING THE MANAGEMENT & SECURITY

  - La DIG de la DGITG tendrá pleno derecho sobre el uso, modificación, mantenimiento y distribución del software una vez entregado.
  - **BEEHIVE SYSTEMS S.A. DE C.V.** realizará la cesión total de derechos sobre la propiedad intelectual desarrollada en cada uno de los proyectos al gobierno del estado de Jalisco.
  - No existirá obligación de continuar contratando los servicios de **BEEHIVE SYSTEMS S.A. DE C.V.** para la operación, soporte, mantenimiento o evolución del software.
  - **BEEHIVE SYSTEMS S.A. DE C.V.** acepta que cualquier práctica que genere dependencia tecnológica más allá del contrato, bloqueo de conocimiento o limitación de uso será considerada un incumplimiento, con posibilidad de ejecución de garantías y fianzas.
  - **BEEHIVE SYSTEMS S.A. DE C.V.**, en los casos de: propuestas técnicas, arquitecturas de software, uso de herramientas de software, desarrollo de software o cualquier otro tipo de servicio o sistema que requiera de licenciamiento, permiso, suscripción, en otros , de manera parcial o total, se compromete a contar con todas las autorizaciones, asumiendo toda la responsabilidad por las posibles violaciones que se causen en materia de patentes, marcas y/o derechos de autor, liberando así a la convocante de cualquier responsabilidad al respecto.
- Transferencia de conocimiento y cesión de derechos:
  - **BEEHIVE SYSTEMS S.A. DE C.V.** ejecutará un proceso formal y completo de transferencia de conocimiento derivado de los servicios realizados a la DIG de la DGITG.
  - **BEEHIVE SYSTEMS S.A. DE C.V.** se compromete a ceder los derechos intelectuales de cualquier producto derivado del servicio a la DIG de la DGITG.
  - La DIG de la DGITG definirá los criterios y condiciones para la correcta transferencia del conocimiento.
- Control del software y repositorio:
  - **BEEHIVE SYSTEMS S.A. DE C.V.** acepta que todo el software, código fuente, documentación y manuales se almacenrán en un repositorio digital tipo GIT bajo control de la DIG de la DGITG y de la DS de la DGTI.
  - **BEEHIVE SYSTEMS S.A. DE C.V.** acepta que la DIG de la DGITG podrá registrar cualquier elemento derivado del contrato como una obra de autoría propia ante instancias nacionales o internacionales.

ATENTAMENTE
15 DE JUNIO DE 2026

ARIEL CARDENAS PEÑA
REPRESENTANTE LEGAL
BEEHIVE SYSTEMS

https://beehivesystems.mx contacto@beehivesystems.mx 33 1588 4412 / 33 8526 3103